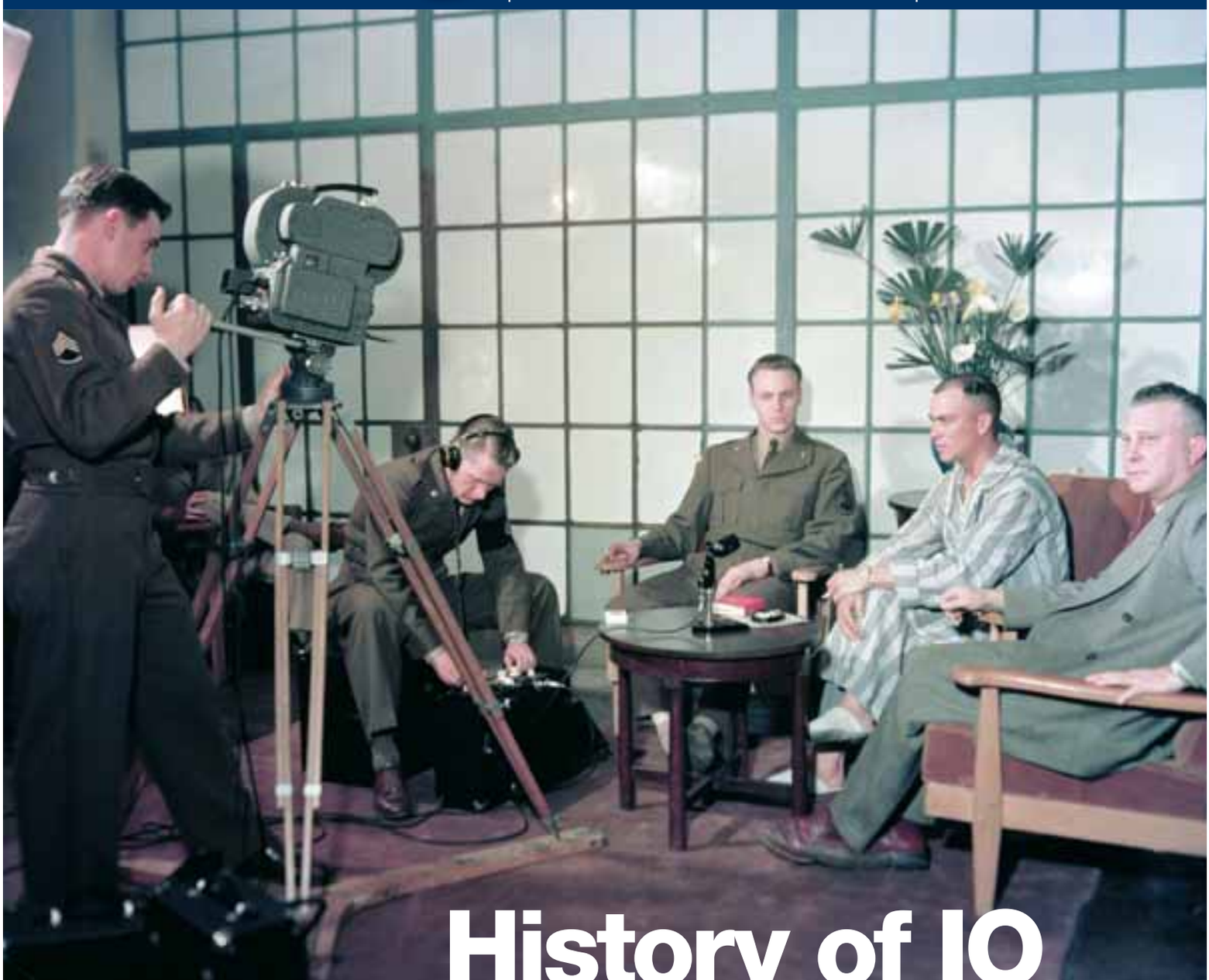
Vol. 1, Issue 2
September 2009

# IO Journal

A publication of the Information Operations Institute



## History of IO

AOC
Association of Old Crows

# |o| about information operations

Information Operations (IO) are activities conducted in or via the information environment with the intent to affect and protect cognition, cognitive processes, information, and the connectivity and processing systems necessary to create and exchange information. IO uses any or all means, in integrated and coordinated means, to create cognitive effects. IO spans the full range of activities in human interaction from person to person through complex, multistate, intercultural, and international communications.

The focus of IO is to affect human beliefs, expectations, decision making and behavior; whether individuals or groups. As a US DoD-originated term, the general intent of conducting IO has been to affect the outcome of military operations; whether to head off combat altogether, undermine the ability of potential opponents to muster effective combat forces, enable the defeat of an opponent, or to ease the stand down from combat operations and transition to peace. The field is not limited to military applications however and the increasing focus of interagency efforts has been on inform, persuade, and influence (IPI) activities supporting nation building and strategic communication beyond the edges of typical military operations. Perhaps the greatest difficulty in IO is identifying the measures of effectiveness for desired outcomes because the means used to achieve them can vary considerably depending on whether the application occurs during peacetime, crisis, pre-hostilities, battle, or transition to peace. An additional significant problem is developing measures of effectiveness that enable evaluation of the efficacy of IO on the perceptions of foreign leaders or groups in crisis.

Whatever the situation, IO is critically dependent on and a voracious consumer of intelligence and technical information. The ability to affect decision makers appropriately, precisely, and legally may require, depending upon the specific effect desired, considerable background information about topics as diverse as the cultural mores of a leader, the internal processing algorithms of radar receivers, telecommunications system protocols, images trusted by various cultures, the extent of foreign intelligence penetration of friendly diplomatic communications, or nearly any other topic describing what someone knows, how they found it out, how reliable they think the information is, and how information is processed.

The tradecraft and expertise of IO continues to evolve through a number of doctrinal and intellectual approaches. Modern IO began with the command and control warfare (C2W) concepts employed during Desert Shield/Storm integrating operations security, electronic warfare, military deception, psychological operations, and kinetic operations. The original C2W term was eventually replaced by information warfare and now IO. The list of disciplines and missions has swelled and contracted over time; sometimes including concepts as diverse as counterintelligence, strategic communication, perception management, and information assurance. The more recent additions to the panoply of IO-associated disciplines are anything using the term "cyber" and the various disciplines involved in interagency IPI.

The debate about the scope of IO and what is 'in' or 'out' has sometimes been referred to by participants as the Definition War. The existence of such vigorous debate is indicative of the importance that modern military and political theorists place on the evolving ability of governments, NGOs, and individuals to effect decision makers at all levels of competition. DoD is once again internally debating a change in the definition intended to reflect the evolving maturity of real world IO and the increasing importance of the integrated application of multiple capabilities to achieve desired soft power outcomes.

Vol. 1, Issue 2 • August 2009

# IO Journal

*U.S. Marine Corps Gunnery Sgt. James Burks, chief of information operations with Regimental Combat Team 3, 2nd Marine Expeditionary Brigade, works from a cot at Forward Operating Base Dwyer, Afghanistan. DoD photo by Sgt. Joseph Breinlinger, U.S. Marine Corps. (Released)*

## |o| Contents



**On the cover:** *Sgt. Bruce Evans (left) and Pfc. Douglas Mandroi, (2nd from left) both of Detroit, Mich., of the Motion Picture Branch, Photographic Division, Far East Command, Signal Service Battalion, 8235th Army Unit, photograph an interview with Sgt. Harry A. Cutting of Kansas City, Kansas (2nd from right) Headquarters Co., 3rd Battalion, 31st Regiment, 7th U.S. Infantry Division, captured by the Communists in Korea, and repatriated under the terms of POW exchange, Operation "Little Switch" at the Tokyo, Army Hospital Annex, Tokyo Japan. Directing the interview for radio, television, Public Information Office, HQ, FEC, for release to the Kansas City Star and television station are Sgt. Robert L. Niermann of Kansas City, Kansas, Radio-TV PIO Division, HQ, FEC, and Mr. Bill Moore, (right) reporter of the Kansas City Star.*




**EDITORIAL & PRODUCTION STAFF**
**Editors:** Joel Harding, Dr. Dan Kuehl
**Design & Layout:** Deb Churchill-Basso

**Submissions:** The ***IO Journal*** welcomes article submissions for consideration. Manuscripts should be of interest to the information operations community and should include proper sourcing with endnotes. All articles are peer reviewed. Direct all submissions to Joel Harding, jharding@crows.org.


Military in uniform attend FREE

# AOC 46th Annual International Symposium and Convention

*Modernizing EW: Balancing Cost and Capability*

## October 18-22, 2009
## Marriott Wardman Park Hotel • Washington, DC

***With a dynamic schedule of sessions and influential keynote speakers, you cannot afford to miss this year's symposium!***

**Sessions:**

***Are We Joint Yet?*** – *Session Chair: Col Marshall Denny, III, USSTRATCOM/JIOWC*
***Advanced Technologies*** – *(two sessions) Session Chairs: Mr. Tracy Johnston, AFRL and Dr. Karl Dahlhauser, OSD/DDR&E*
***International EW – A US Perspective*** – *Session Chair: Mr. Kermit Quick, AOC President*
***Industry Leader Roundtable*** – *Session Chair: Mr. John Knowles, Editor, JED*
***IO and EW: Simply Siblings or Conjoined Twins*** – *Session Chair: CAPT Gregg K. Smith, Naval IO Command Norfolk*
***Institutionalizing Irregular Warfare*** – *Session Chair: Mr. Anthony Lisuzzo, Intelligence and Information Warfare Directorate, US Army*
***Congressional and Government Leadership for the Future of EW*** – *Honorary Session Chair: The Honorable Joseph R. Pitts, US House of Representatives (PA-16)*
***EW in 2030*** – *Session Chair: Col Chris Glaze, USAF (Ret.), L-3 Command and Control Systems & Software*

More than 80 EW and SIGINT exhibitors have already booked their space and more are expected!

*DON'T MISS THE CHANCE TO LEARN, NETWORK, MEET POTENTIAL CUSTOMERS AND IDENTIFY BUSINESS OPPORTUNITIES THAT ARE CRITICAL TO THE FUTURE OF YOUR BUSINESS.*

***Visit www.crows.org to register, purchase an exhibit booth or to read more about the convention.***

***Register online at www.crows.org***

## *Current Sponsors*

Platinum: BAE SYSTEMS, elt

Gold: Raytheon, ITT, SELEX Sensors and Airborne Systems Inc., Northrop Grumman, Rockwell Collins

Silver: AAI Textron Systems, Lockheed Martin, General Dynamics, TERMA, Anaren, COBHAM, L3

Bronze: Symetrics Industries, SRC Tec, Esterline, e2v

# New Developments in IO

By Dr. Dan Kuehl

This second issue of the Information Operations Journal arrives with the Information Operations community on the verge of several critical new developments. The recent World Wide Information Operations conference, again hosted by the Joint Staff's J-39, Brigadier General Rowayne Schatz, hinted at some of them.

The IO sub-panel to the ongoing Quadrennial Defense Review is wrapping up its work, including a fundamental relook at how we define IO. It is clear that the current definition of IO, first formulated in the 2003 "Information Operations Roadmap" and formalized in the 2006 version of Joint Pub 3-13, is on the way out. Many in our IO community have felt that the focus on "5 core competencies" was dysfunctional at best and a spur to fragmentation at worst, and virtually no one will shed a tear at its passing. While we don't know yet precisely what a new definition will include, the information environment may well occupy a central place in a new definition that emphasizes integration and coordination of effects. While many in our community have decried what they perceive as a useless focus on definitions, arguing that this effort diverts time and attention from real IO, remember that what we consider IO to be and how we resource and do it is determined by how we define it. This is a critical task, and the QDR IO panel is to be commended for its work advancing this process.

Doctrinal change is everywhere. Joint Pub 3-13 is due to begin the revision process, although a new one is at least a year away and likely won't be started until the QDR IO Panel has completed its work. In the Services, both the Air Force and Army have doctrinal efforts underway. The Army is essentially starting from scratch after last year's effort to revise FM 3-13 failed. The Air Force halted work on its IO doctrine, Air Force Doctrine Document 2-5, so that work on its new Cyberspace doctrine, AFDD 2-11, could begin, although neither has been approved. The importance of doctrine – another topic that many argue as irrelevant – is that doctrine is how military forces shape new operational concepts, which are at the heart of any "revolution in military affairs".

Organizationally, IO is being pushed forward by developments in Cyberspace. The Marine Corps has activated its new Marine Corps Information Operations Center at Quantico, the Air Force is creating a new 24th Air Force at Lackland AFB, the Navy is standing up Fleet Cyber Command and 10th Fleet, and of course, US Strategic Command has been directed to establish a new unified Cyber Command as a subordinate unit replacing the Joint Force Component Command-Network Warfare and the Joint Task Force for Global Network Operations. As with doctrinal change, organizational change is another critical aspect of any RMA.

Two issues inseparable from IO have been in the news consistently over the past few months, cyberspace and strategic communication. While the President's cyber review effort has not (yet) led to appointment of a so-called "cyber czar", the news media have carried a seemingly-endless series of stories centered on cyberspace. Whether focusing on cyber privacy, or hacking attacks from potentially hostile countries, or interagency organizational developments and "cyberturf" fights, the coverage of cyber issues is evidence of its strategic criticality. Strategic communication is certainly not far behind in terms of media coverage, if it's behind at all. Within the IO community, the past several World Wide IO conferences have been remarkable for the amount of discussion – seemingly half of the conference content--devoted to issues involving influence and strategic communication. Stories about the "softer side" of IO abound, from *The New York Times to Joint Force Quarterly*. This year's WWIO conference was a demonstration of this "dual nature" of IO, with major conference segments and very senior speakers/panelists devoted to these two sets of issues.

As Austin Branch, the Senior Advisor for IO Strategy and Plans in USD/I, said at the most recent WWIO conference, IO has certainly "arrived." We're not a niche capability or community, and the effects we create and offer to the national military and political leadership are crucial and at times decisive. It's a good time to be an "information warrior!"


## World Wide EW Infrastructure Conference

**October 6-8, 2009**
Atlanta, GA

**Call for Papers and Presenters**
The AOC is soliciting original, unclassified papers that address technical capabilities within the international EW community, focused on the following topics: Sustainment, Development, Integration, Transformation.

For submission information, visit **www.crows.org**.

## Fall 2009 Navy EWIIP Conference

**November 3-5, 2009**
Little Creek Naval Station
Virginia Beach, VA

Conference Chairman: **CAPT Brian Hinkley**
Last year this was a very successful conference with direct impact on Navy programs. Sign-up early so you don't miss your chance to take part in the discussions!

***Upcoming AOC Conferences:***

## Operationalizing Intelligence in Electronic Warfare for the 21st Century Conference

**December 1-3**
NASIC, Wright Patterson, AFB
Dayton, OH

The conference will address the need to improve the lines of communication between the intelligence and the operational EW communities. This is particularly true for communicating warfighter needs across the electromagnetic spectrum to intel and delivering intel products to the warfighter.

**Call for Papers**
Previously unpublished contributions across a broad range of topics in intelligence support across the electromagnetic spectrum are solicited.

AOC
Low Probability of Intercept, ELINT/SIGINT
Naval Post Graduate School, Monterey, CA
November 17-19, 2009

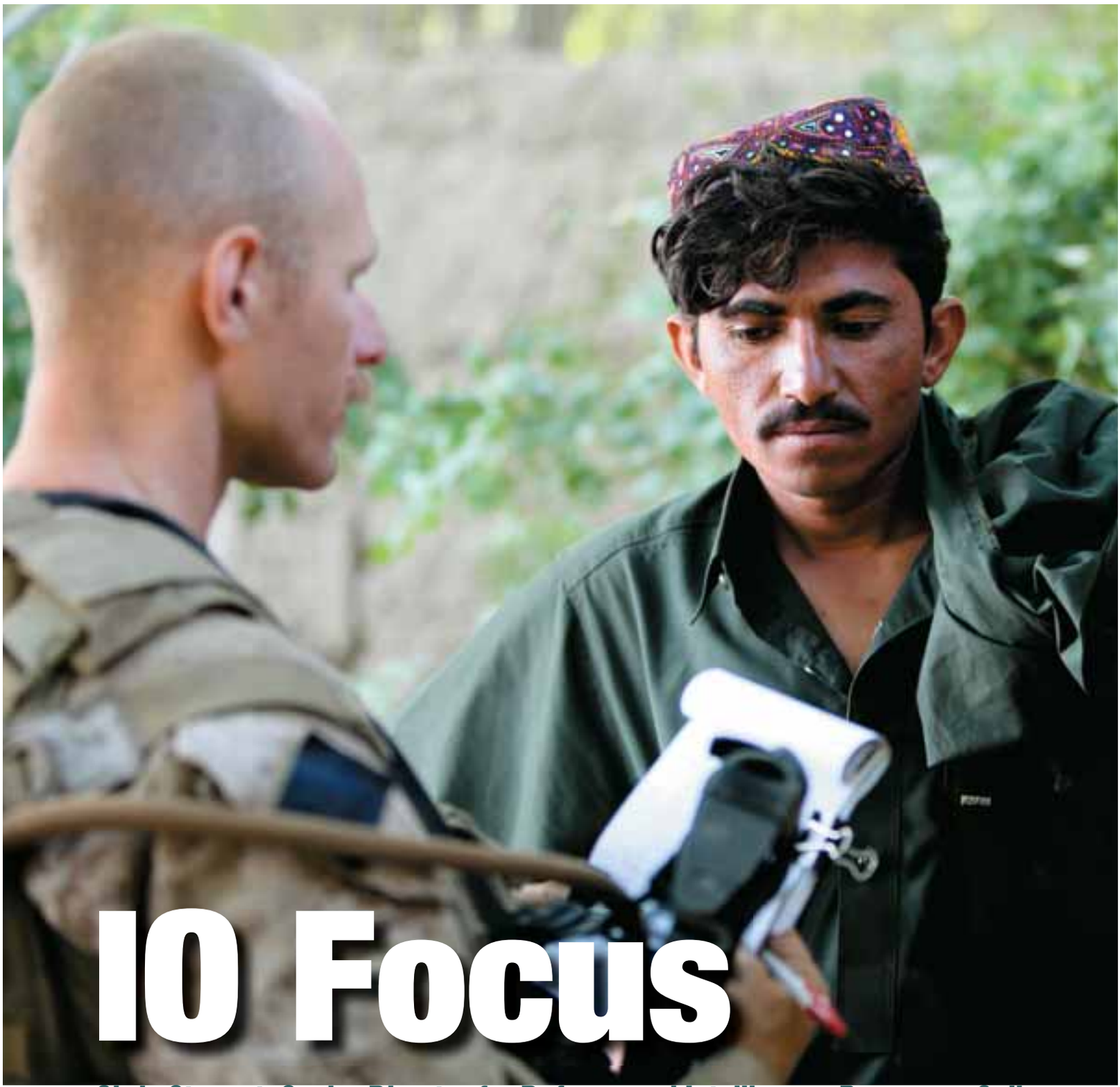
## Low Probability of Intercept, ELINT/SIGINT

**Call for Papers Now Available**
**November 17-19**
Naval Post Graduate School, Monterey, CA

***Interested in sponsoring a conference? Contact Kent Barker at 703-445-7798 or e-mail barker@crows.org***

***Single conference sponsorship or conference packages available!***

***For more information visit www.crows.org***



# IO Focus

## Chris Stewart, Senior Director for Defense and Intelligence Programs, Gallup

**By Bill Canter**

You meet the most interesting people in the Information Operations business. This summer, Chris Stewart, Senior Director for Defense and Intelligence Programs at the Gallup organization, whose work in Iraq and Afghanistan have positioned him to have access to and share an understanding of the media landscape in that part of the world, dropped by my office. I had the unique opportunity to discuss a number of items germane to the current state of IO.

*Chris Stewart*

**Bill Canter: Chris, National Director of Intelligence Dennis Blair said: "The United States needs to improve its level of intelligence support to military operations in Afghanistan. The United States lacks a deep understanding of local power structures in Afghanistan and of**

*U.S. Marine Corps 1st Lt. Michael Kuiper, with 1st Battalion, 5th Marine Regiment, talks with an Afghan man during a civil affairs group patrol in the Nawa District of Helmand Province, Afghanistan, July 19.*

**the militants' operation along that nation's border with Pakistan." Has Gallup's activities in the region borne this out?**

**Chris Stewart:** Let me start by addressing the information environment in Afghanistan vs. Iraq. I can set the stage by saying that there is not necessarily a mass media strategy for Afghanistan. It's a convoluted market; very difficult to work in, and through it you'll get a flavor of the challenges that an IO practitioner will face in the Afghanistan theatre of operations.

Now, television is almost universal throughout the Arab world. We find that 95 percent of Iraqis have terrestrial television or satellite broadcasting in their homes. Half that rate exists in Afghanistan today. Fresh data [as of December 2008] tell us that cell phone penetration is rather high in Afghanistan, but it's not an internet market at this point. That said, there are some strategies to influence key leaders through internet activity, but it's not a dominant means of communicating with the mass market of Afghanistan.

Probably the largest challenge is the low literacy rate — about a quarter of the Afghan population can actually read. So, this creates a tremendous challenge to our communicators who are putting products out on the street or passing out leaflets or using electronic communications. [O]ne of the more surprising facts is that only 13 percent of females are literate in Afghanistan. There's a huge variation by sect, by province, by language, by those [who] speak Dari and those [who] speak Pashto. And down in the south where we've got so many of the battles, you only have about a nine percent literacy rate.

There's a huge variation across Afghanistan with respect to the television environment by sect, by ethnicity and by geography but, basically speaking, the country is on par with many states in Sub-Saharan Africa. Of about half of the Afghan households today that do have television, only about four in 10 of those are Pashtun, with about 14 percent down in the southwest. Obviously, it's not a medium that we can rely on to communicate with target audiences.

[W]e have seen an increase in television penetration, particularly in the [past] couple of years, but it's still not necessarily a viable medium at this time.

This is a radio market. Our data show that about 83 to 85 percent of Afghans rely on the radio as their major source of news and information.

One of the complications, though, is when you dive in and really ask individuals what are their sources of information [are]; it's very often their malaks, their shuras, their mullahs and other local tribal leaders. So, the additional challenge in communicating with the target audience is that you've got a filter. Those key leaders are filtering the messages coming through radio, print or TV. It creates an extra challenge in ensuring that the message is delivered. It's the old telephone game, you know: I pass this message to one person, and then it gets convoluted and passed to the next.

Interesting to note: we've found fairly high media confidence in Afghanistan. About one in two Afghans report that they have confidence in the media. This compares to Iraq, where only about one in three Iraqis feel that there's confidence in the media. This is up about 10 percent in

the [past[ two years, so there is growing confidence in the media. The challenge, though, is that in the areas that we're targeting — in the east and the south — there is much less confidence in the media.

**Bill Canter: Information like this is why we have turned to Gallup for years. How did Gallup come to put people on the ground in Afghanistan?**

**Chris Stewart:** A couple years ago, the former Secretary of Defense was asked in a press conference, "What do you think the support levels are amongst the Afghan people for the Taliban?" And his response to the media was, "Hell if I know — it's not like we can go out and do a Gallup poll!" Well, that motivates folks like us, which enables me to have some of the answers for you here today.

In Iraq, we've got about 1,100 local nationals [who] work for us. We were the first on the ground in August 2003. Regardless of location, a lot of work went into ensuring that the questions that we ask were neutral and unbiased, and understandable by the respondents, particularly in places like Afghanistan where you've got such low literacy rates. Not to mention — or not to avoid — the whole issue of denied areas. You know, we've had interviewers that have been kidnapped by Taliban members; we've had interviewers beaten. It is a major logistical challenge to be able to go in and, in some cases, interviewers are negotiating with tribal elders or even Taliban leaders to get into those communities to ask those questions.

Our most recent data report that about 8 to10 percent of the Afghan population thinks that the Taliban exert a negative influence. So they haven't necessarily won the war in terms of the hearts and minds. However, there are some troubling areas with respect to the south.

Those in the south [who] say that the Taliban has a positive influence have doubled the national view in terms of support for the Taliban. The data are from Helmand, Ghazni and even down in Khandahar.

We recently asked the Afghan public [about their views… since the Taliban era in 2001. I think this is a positive story; six in 10 think [the situation is better now], and we've got another quarter of the population that thinks it's about the same. Only about 20 percent of the population actually believes that things are worse since the fall of the Taliban. And again, we find most of those in the south and in the east.

**Bill Canter: Media coverage of casualties is as varied as the many outlets presenting news and information about Afghanistan. Accepting that there are three basic audiences — the general population of Afghanistan, the Taliban and the western world — how do you frame the diversity of coverage of this component of the current conflict?**

**Chris Stewart:** We've asked this question in probably 40 predominantly Muslim states and in non-Muslim states, as well. And when we look at the response … 92 percent of Iraqis say [targeting civilians is] never, NEVER justified.

[T]he findings in Afghanistan [are that] it's a much different picture. [A]bout 64 percent say that it's never justified. The central region is very strong in their opinions: seven in 10 say that it's never justified. But then, when we go to the south or the east, we see much greater support levels that it's okay or sometimes, or it depends [on] whether military attacks on civilians are okay. I think it's a fascinating response, and I think there's a lot behind it that we all need to better understand.

**Bill Canter: There are other sensitive areas that, even if given ample time to prepare, one might not have the best possible answer. I am thinking here of the gender equality issue.**

**Chris Stewart:** I'm not so sure that I think it's more important to go out and understand what the women want to do. A few years ago, there was a U.S. government official who felt that all Saudi women wanted to drive. Well, a lot of them *didn't* want to drive; they got chauffeured around and were happy — so, I think it's important to go ask the questions and better understand a localized point of view . . . the local environment.

We just did a real interesting analysis on 148 countries around the world. Of those countries that had greater connectivity — television, cell phones, internet — we found much lower support level towards the United States.

I'm not saying that the outcome that we're trying to reach is that everybody loves us, but where our strongest support levels are, in Sub-Saharan Africa states, roughly about one in two Afghans are supportive of the [United States]. And, it's an interesting problem that the more wired people are, the more information they're getting about the [United States].

You know, it's largely about our policies, and it's about our personalities. I'm an advocate for expanding the communication infrastructure. But there are effects to that, which may keep it from happening, and which aren't always going to be positive for us.

***Christopher Stewart*** *is the Senior Director, Defense and Intelligence Programs for The Gallup Organization. He also plays a senior leadership role as a strategic advisor for Gallup's 148-country attitude and behavior tracking program — The Gallup World Poll. Mr. Stewart previously served for 10 years as Regional Managing Partner of Gallup's Asia Pacific Division, where he was responsible for managing Gallup's seventeen offices in the Asia Pacific region. He remains a director of Gallup companies in Singapore, Thailand, Australia, Malaysia, Hong Kong and India, and as the general director of Gallup Institute LLC, a Russian subsidiary of Gallup, Inc.*

***Bill Canter*** *serves as Vice President, Media, Marketing and Communications at SOS International, Ltd., a privately-owned operations support company now in its 20th year supporting contracts covering information engagement, intelligence solutions and stability operations for a list of notable U.S. government and commercial clients. Mr. Canter is a Peabody and Emmy-award-winning broadcast journalist with more than 35 years of industry credits.*

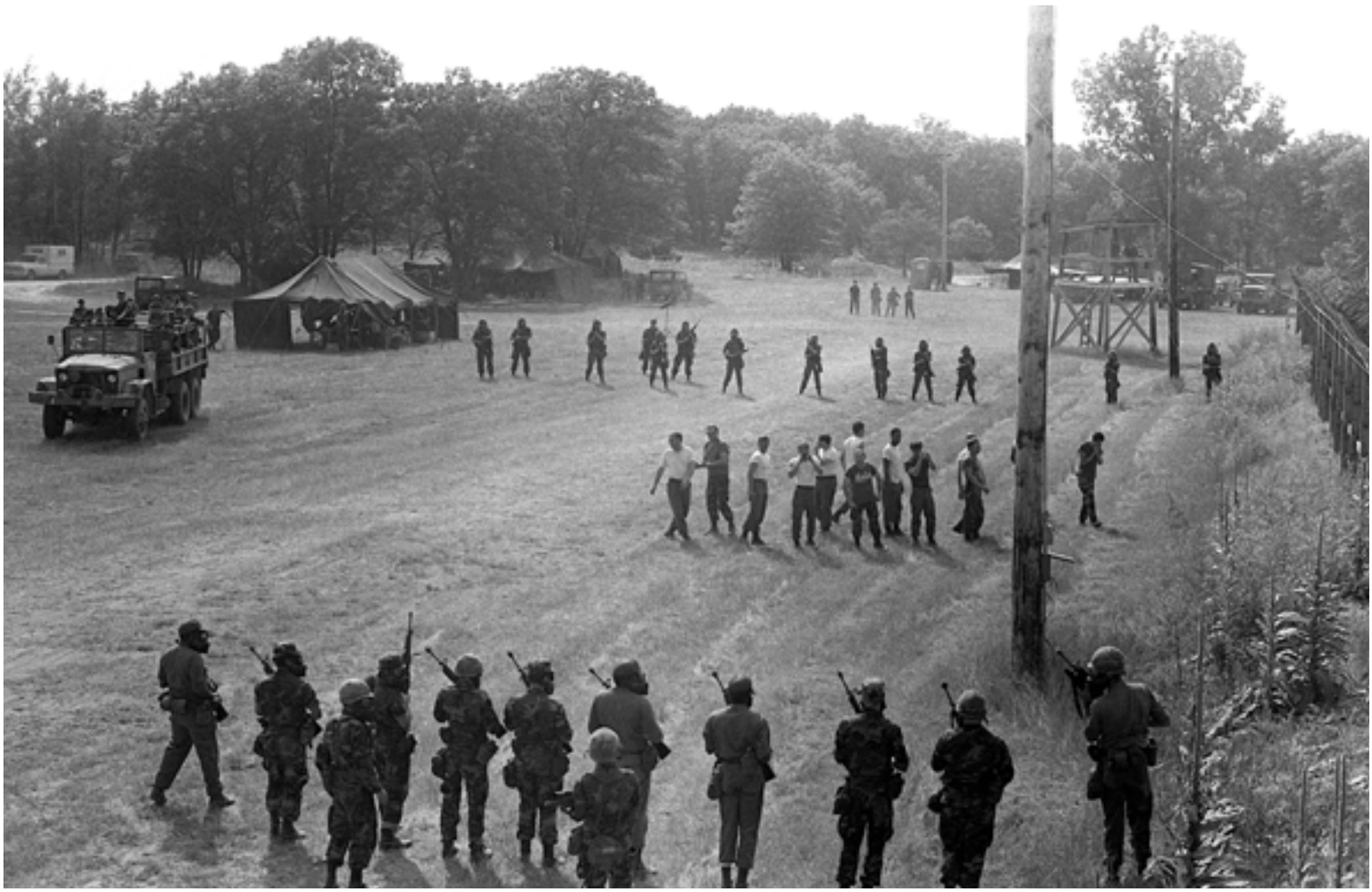
*Tech. Sgt. Barry Hein, foreground, an electronic communication systems operator, coordinates a broadcast mission from an EC-130E Volant Solo aircraft of the 193rd Special Operations Group (Pennsylvania Air National Guard).*

# Information Operations: Where Has It Gone?

**By Nicoline K. Jaramillo**

The United States Army is working to revise the doctrine for information operations; therefore, they are rewriting the field manual that defines the breadth and depth of use for information as an element of combat power in full spectrum operations. The Army has moved away from the use of information operations (IO) as a strategy and moved to using five Information Tasks (see **Figure 1**) (Army, 2008) to cover the breadth of application within military missions; however, there is considerable pushback from deployed units and the career field. Currently, the Department of Defense (DoD) uses the term Information Operations (IO) to describe the application of information as an element of combat power (Shelton, 2006).

The Army and Joint publications have doctrinally defined IO as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making



*Members of the 13th Psychological Operations Battalion undergo riot control training at a mock prisoner of war camp at Fort McCoy, July 1982. Photo by SSGT Jan Caeotte.*

while protecting our own" (Shelton, 2006 & Army, 2008). Joint Publication (JP) 3-13 (2006) further explains that the primary goal of IO, at all levels, is to successfully synchronize and deconflict planning and operational efforts in order to achieve information superiority.

Information superiority is "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." The ability to gain information superiority is dependent on knowing the operational environment that the commander is operating within and how that environment effects mission accomplishment. The battlefield has undergone many changes with the advancement of technology and the changes made to conduct operations (Army, 2008).

Since the early 1990's there has been a move by the United States Government (USG) to change the way the military executes operations (Armistead, 2004 & Berkowitz, 2003). In order to leverage the technology and all aspects of the operational environment the military strives to capitalize on the power associated with information and information systems (Armistead, 2004 & McClausland, 2000). There does not appear to be a lack of consensus that IO, or a similar strategy is needed; however, there does not appear to be a clear 'business plan' for the continued development, implementation, and sustainment of an IO strategy.

The core capabilities, as well as the related and supporting activities are not new to military operations; however, the strategy known as IO was introduced in 1996 (Hiemstra, 1999). Due to the lack of clear guidance and clarity leaders have been left to determine how IO fits within operations and determine the best way to define information's operational value (CALL, 2008).

Trent and Doty (2005) equated the value of information to the civilian concept of marketing communications for their commander. Within marketing communications the organization is trying to influence their target audience to purchase their product or brand name. The concept for IO is similar. An IO planner, or staff, is interested in developing an operational plan that will influence adversarial decision-making in favor of friendly mission accomplishment. This is the same process that PSYOP has used since World War II when determining the best messages to influence their target populations (Trent & Doty, 2005).

Through the late 1970's and into the first part of 1980, the Department of Defense (DoD) used the term command, control and communications countermeasures (C3CM), which hailed with much confusion and mislabeling. The initial utilization of C3CM was intended to incorporate a new philosophy of thinking into tactics and strategy for employing military power. Ultimately, it was considered a "warfighting technique" necessary to accomplish military missions. It is important to note; however, that C3CM was not simply about electronic warfare, hardware, and systems, it was about understanding where the adversary's command, control, and communications

| Task | Information Engagement | Command and Control Warfare | Information Protection | Operations Security | Military Deception |
|---|---|---|---|---|---|
| Intended Effects | - Inform and educate internal and external publics<br>- Influence the behavior of target audiences | - Degrade, disrupt, and exploit enemy command and control | - Protect friendly computer networks and communication means | - Deny vital intelligence on friendly forces to hostile collection | - Confuse enemy decision makers |
| Capabilities | -Leader and Soldier Engagements<br>- Public Affairs<br>- Psychological Operations<br>- Combat Camera<br>- Strategic Communication and Defense Support to Public Diplomacy | -Physical Attack<br>- Electronic Attack<br>- Electronic Warfare Support<br>- Computer Network Attack<br>- Computer Network Exploitation | -Information Assurance<br>- Computer Network Defense<br>- Electronic Protection | -Operations Security<br>- Physical Security<br>- Counterintel-ligence | - Military Deception |

*Figure 1: Army Information Tasks — This figure displays the Army's five information tasks with the associated capabilities and the desired effects. This figure was copied from FM 3-0 (2008), p. 7-3.*

capabilities were susceptible to attack, destruction, deception, degradation, or denial while still protecting friendly capabilities (Smith, 1983; Armistead, 2004).

At the onset of the concepts the military was faced with the problem of "devis[ing] meaningful measures of effectiveness" (p. 51); therefore, the inculcation of C3CM concepts into military operations was slow. In 1983, C3CM was defined as "the integrated use of operations security, military deception, jamming, and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary C3 capabilities and to protect friendly C3 against such actions" (p. 51). The focus of C3CM was on understanding how the enemy's command, control and communications were vulnerable to friendly capabilities and leveraging friendly assets to effect adversary decision-making. Much like today, staffs had a problem with C3CM being treated as an ad hoc capability and fought for early integration of the capabilities into the military planning process (Smith, 1983). Over time, as the capabilities and technologies have improved, the conceptual framework for utilizing information as a force multiplier has also changed (see **Figure 2**), as have the definitions and associated terminology.

Since introducing information as a force multiplier, it has been the intent of military leadership and theorists to provide commanders with a means of disrupting or destroying enemy command and control capabilities or to deceive the enemy about the true nature of friendly operations in order to change force ratios at a minimal cost (Armistead, 2004). C3CM was for operators and intended to provide a strategy for achieving an operational advantage; however, it was not intended to be synonymous with electronic warfare, hardware, or systems (Smith, 1983). C3CM provided "the basic concept" and units possessed the necessary mechanisms; however, the top down emphasis required to energize planners "to orchestrate this multifaceted concept" was lacking (Smith, 1983, p. 53).

The next major change came with the publication of C2CM strategy (Army, 1992) and the Chairman of Joint Chiefs Memorandum on Command and Control Warfare (Macke, 1993). With these publications the Army rescinded the use of C3CM and adopted the term command and control countermeasures (C2CM). C2CM was "the integrated use of lethal and non-lethal means, OPSEC, and military deception against the enemy's command and control (C2) capabilities" (Army, 1992, p1). The Army chose to remove communications from the C3CM concept because they did not believe it was the focus of the command and control strategy they were trying to employ. While the Army recognized the need for communications and understood its intrinsic value, the belief was that taking direct or indirect action on the enemy's command and control networks would delay and/or deny the enemy's ability to employ concentrated combat power (Army, 1992).

The intent of the refocused concept was to use battlefield operating systems to influence the adversary's command and control functions in order to "delay or deny the proper concentration of combat power" (Army, 1992, p. 1). The regulation focused on defining how commanders could use C2CM to counter adversary collection efforts and to formulate operational plans. The primary effort of C2CM was focused on collection capabilities; more specifically, it took a technical, electronic approach to delaying, denying, destroying, or disrupting adversary intelligence reporting and control of the commander over adversarial forces (Army, 1992; Macke, 1993).

As the desire to effect command and control became more pervasive and technological capabilities began to catch-up with the operational concepts, Joint policy adopted the term command and control warfare (C2W) (Armistead, 2004). In 1993, C2W was defined as "the integrated use of operations security (OPSEC), military deception (MILDEC), psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions (Macke, 1993). The adoption of C2W was initially prompted by implementation of information warfare as military strategy on the battlefield by the DoD Directive TS 3600.1 in 1993 (Armistead, 2004). The primary goal of C2W was to "decapitate the enemy's command structure from its body of combat forces" (Macke, 1993, p. 3).

The DoD Directive was followed by the Chairman of the Joint Chiefs of Staff document (1993) on C2W laying out, for the first time, an unclassified explanation of the capabilities available. C2W had offensive (Counter-C2) and defensive (C2-Protection) components, both intended to support the commander in mission accomplishment. As the geographical space of a unit's battlefield grew and technology increased the speed at which operations occurred reinforced the value of accurate and timely information for decision-making on both sides. Successful integration of C2W capabilities on the battlefield provided an operational advantage to commanders by getting them the information first (Macke, 1993). However, the DoD Directive (DoDD) TS3600.1 discussing information warfare doctrine was much broader than just this idea of C2W (Armistead, 2004).

In 1996, FM 3-13 incorporated the larger DoD information warfare strategy, defined as "a feature of military conflict where information systems are attacked or defended, directly or indirectly as a means to dominate, degrade, or destroy, or protect or preserve data, knowledge, beliefs or combat power

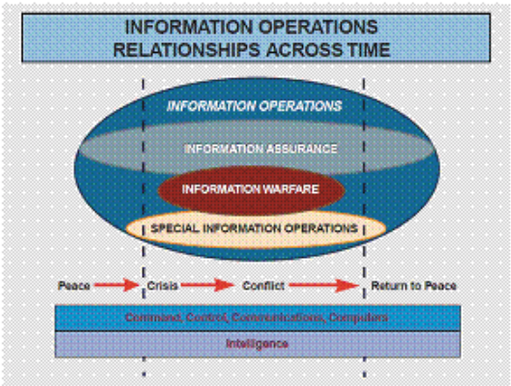



*Figure 2: Conceptual Integration of IO — This figure provides a graphical depiction of a notional timeline of engagement across all core and supporting capabilities. This is a figure copied from JP 3-13 (1998), p. II-8.*

potential" (Hawkins, 1997, p. 2) in a more overarching doctrine, which was intended for use during peace operations by introducing information operations (Army, 1996). This "doctrine was heavy on theory and light on practice, and definitions tended to be long and repetitive" (Wright, 2001, p. 30). The inability to successfully integrate and coordinate these activities cedes the operational advantage to the adversary and hinders the ability of friendly commanders to leverage information as an element of combat power (Army, 1996).

In FM 3-13 (1996) the Army attempted to capture the broader sense of information as a force multiplier by maintaining the use of the term C2W within the broader concept of information operations. This manual emphasized a need to embrace "a new era characterized by the accelerating growth of information, information sources, and information dissemination capabilities supported by information technology," commonly referred to as the Information Age (Army, 1996, p. iv). FM 100-6 (1996) discussed "integrat[ing] all aspects of information to accomplish the full potential for enhancing the conduct of military operations" (Army, 1996, p. 2-3). FM 100-6 (1996) defined information operations as "continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision [making] capabilities" (Army, 1996, p. 2-3).

FM 100-6 (1996) was focused on providing the warfighter with an understanding of the operating environment through an understanding of the global and military information environments. The manual explains the value of information in regards to the cognitive hierarchy of individuals and links deterrence of adversary actions to the successful use of information. The Army adopted the term information operations as their means of meeting the DoD requirement for executing the information warfare strategy, defined as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks" (Army, 1996, p. 2-2).

The initial concept of information operations had "three interrelated components…: operations, relevant information and intelligence (RII), and information systems (INFOSYS)" (Army, 1996, p. 2-3). Operations were composed of C2W, civil affairs, and public affairs, which were capabilities the Army used to gain and maintain information dominance. In the 1996 doctrine, "C2W [was] the warfighting application of IW in military operations" (p. 2-4) with the goal of influencing, denying, degrading, or destroying adversary command and control capabilities. Civil affairs operations provided commanders a tool to interface with critical actors and influenced the global information environment. Civil affairs activities were used to "maintain, influence, or exploit relations among military forces, civil authorities, and the civilian populace in an [area of operation] to facilitate military operations" (p. 2-5). Public affairs operations provided the commander with a reliable and dedicated capability for dealing with news media, contributing to public debate and shaping public opinion. Under the 1996 doctrine, public affairs officers were responsible for monitoring public perceptions, as well as developing and disseminating objective messages about military operations (Army, 1996).

Relevant information and intelligence was centrally involved in the collection and analysis of information in order to disseminate useful and timely intelligence to support the commander's decision-making and execution. "[Information systems] collect, process, and disseminate information relating to current and future operations" (p. 2-6), this was the means by which the commander and his staff could monitor the current situation, synchronize operations, integrate the battlefield operating systems, coordinate joint support, update targeting parameters, and control operations throughout the battlefield (Army, 1996). Overall the doctrinal concepts within FM 100-6 appear to have been focused on influencing a hierarchical, highly structured adversary and the commanders use of information systems and intelligence; however, the need to deal with the civilian population was a result of military operations, not as a means of shaping the operational environment.

In 1998, the Joint community continued the use of information operations as an overarching strategy, with a differentiation between offensive IO and defensive IO. JP 3-13 (1998) defined information operations as "actions taken to affect adversary information and information systems while defending one's own information and information systems" (p. I-9). Overall, the publication had adopted the Army's broader utilization of IO as a strategy for including information as a force multiplier.

JP 3-13, Information Operations (1998) explained information operations as a strategy to integrate capabilities and activities into an operation in order to achieve national military objectives (Shelton, 1998).

As part of the IO strategy, JP 3-13 (1998) defined a split between offensive and defensive IO capabilities and activities; initially identifying fifteen various IO capabilities and related activities. Offensive IO assigned and supporting capabilities were intended to affect adversary decision-making and pro-

mote achieving specified objectives. Defensive IO used the assigned and supporting capabilities to protect friendly assets, decision-making processes, and activities from adversarial detection to assist in mission accomplishment. Through these changes the focus of IO remained on influencing a hierarchically structured adversary's decision-making by attacking their information and information systems, which required highly effective interaction and communication between command, control and intelligence support capabilities (Sheldon, 1998).

In 2001, Wright published an article in Military Review discussing information operations. Wright (2001) made the argument that the 1998 joint doctrine was a step in the right direction and provided Army doctrine with a better venue for the integration of IO capabilities. It was with this in mind and the need to provide commanders with an IO coordinator that the second Army IO manual was eventually written. In his conclusions he noted that the Army had successfully used the individual elements of IO with great success; however, the true benefit and full potential could only be achieved when the individual capabilities were integrated together for a synergistic effects (Wright, 2001).

As units struggled with the need to update the doctrine and clarify the applicability of information operations, Secretary of Defense Donald Rumsfeld, published the Information Operations Roadmap (2003). The roadmap provided DoD with guidance and a vision for advancing the goal of making information operations a core military competency and reinforced the 2001 Quadrennial Defense Review assessment that IO was one of six critical operational goals (Rumsfeld, 2003). As a core competency services were directed to establish career forces and develop training programs to enhance combatant commander's capabilities to successfully utilize information as an element of combat power (Wolfowitz, 2001 & Rumsfeld, 2003).

The "primary focus of IO was on decision-makers; the information they acquire and use to make decisions, the information they generate in making decisions and the full range of systems and organizations in handling, processing and implementing this information" (Wolfowitz, 2001, p. 2). The roadmap defined the core capabilities of IO as central to operations, stipulating that the five capabilities of PSYOP, CNO, EW, OPSEC, and MILDEC were interdependent and required close integration to successfully achieve desired effects. The roadmap also supported the necessity to identify supporting and related activities for the successful integration of IO. The document was the first step in introducing the five core capabilities of IO, adopting the C2W definition as IO and rescinding the use of the terms C2W and information warfare (Rumsfeld, 2003).

The 2003 Roadmap provided a common framework from which each of the services were to continue developing their IO capabilities. However, the primary focus of IO continued to be on "degrading an adversary's decision-making process while preserving our own" (Rumsfeld, 2003, p. 10). This was to be achieved by disrupting an adversary's unity of command, protecting friendly plans while misdirecting adversaries, and controlling adversary communications and networks. Information operations were established as a full time endeavor and necessary throughout the full spectrum of operations. In 2003, the roadmap redefined IO as "the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making

*While on a two week tour of active duty, Brig. Gen. James Stewart, Deputy Chief of Information USAF, visited Orlando AFB where he was briefed on rescue and photographic operations. Here, Master Sgt. George Weir, motion picture cameraman of the 1365th Photo Squadron, shows Gen. Stewart the operation of the control box in the "Solarama Room." Gen. Stewart is sitting next to an Arriflex 35mm motion picture camera with a 100 load.*

while protecting our own" (Rumsfeld, 2003, p. 11). Interestingly, this seems to have taken the doctrinal concept back a step, once again narrowing the focus and capability back to a force multiplier used during conflict and not a broader concept more easily applied throughout full spectrum operations, more specifically during peacetime, and decreases the focus on civilian populations as a tool for shaping the environment.

A month after the publication of the IO Roadmap, FM 3-13 (2003) was published, establishing information as an element of combat power. The manual changes the initial IO construct to meet the offensive and defensive components defined in JP 3-13 (1998) and adopted a fourth definition of IO. FM 3-13 (2003) defines IO as "the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making" (Army, 2003, p. 1-13). The manual opens with a discussion of IO as an integrating strategy intended to bring together a set of "previously separate functions as IO elements and related activities" (p. 1-1) to affect the adversary's decision-making capabilities while protecting our own (FM 3-13, 2003). Instead of approaching the information aspects of the environment through multiple lens, the doctrine started defining a single information environment consisting of three dimensions (cognitive, informational, and physical). The military actions taken within the information environment are intended to assist commanders in achieving "an operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same" (p. 1-10), called information superiority. The initial 1996 concept of relevant information appeared to have moved to the intelligence, surveillance, and reconnaissance (ISR) contributions of the information superiority construct (Army, 2003).

In 2003, the Army IO construct defined five core elements (EW, CNO, PSYOP, OPSEC, and MILDEC), six supporting elements (physical destruction, information assurance, physical security, counterintelligence, counterdeception, and counterpropaganda), and two related activities (civil affairs and public affairs) (Army, 2003). Achieving an information advantage through the use of offensive IO capabilities aided commanders in destroying, disrupting, degrading, denying, deceiving, exploiting, and influencing. Protection, detection, restoration, and response were the effects achieved through the application of defensive IO capabilities. Part two and the appendices of the manual provided several tactics, techniques, and pro-

cedures to aid commanders and their staffs in planning and executing IO (Army, 2003).

Currently joint doctrine defines information operations as "the integrated employment of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own" (Shelton, 2006, p. I-1). JP 3-13 (2006) further explains the primary goal of IO, at all levels, is to successfully synchronize and deconflict planning and operational efforts within the process of achieving information superiority. Joint doctrine correlates the ability to gain information superiority with the ability to understand and visualize the information environment and how the information environment effects the larger operational environment for mission accomplishment. JP 3-0 (2006) defines the operational environment as "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander" (Pace, 2006, p. xvi).

JP 3-13 (2006) refocuses the integrating ability of IO by dropping the division between offensive and defensive IO capabilities. The approach adopted in JP 3-13 focuses on the use of full spectrum operations, treating offense, defense, and stability or civil support operations on par with one another. In 2006, the publication also made some changes to the supporting and related activities. Of most interest are the introduction of Combat Camera as a supporting capability and the addition of defense support to public diplomacy to related activities. However, the intent and utility of IO as an integrating strategy remains the focus of the construct with the intent of influencing, disrupting, corrupting or usurping adversarial decision making while protecting friendly capabilities (Shelton, 2006).

Cox (2006) recommends adjusting the approach of IO to more clearly define the application within military operations by adopting by coordinating the functions of influencing, informing, attacking, and protecting to produces effects on the battlefield versus "merely adding the results of the individual functions together" (Cox, 2006, p. 3). In his proposal, influencing would be the process of changing behaviors of a target audience and informing would be the actions taken to provide information to target audiences about US activities, intentions and operations. The effects of neutralizing, suppressing, degrading, or destroying adversary IO capabilities are achieved through the application of the attack function; while using the protection function to safeguard friendly IO capabilities (Cox, 2006).

Cox (2006), continues the consistency with previous publications, concluding that IO "from conception… was always intended to be integrated into a unit's operations" (p. 55). The first conclusion drawn in the article emphasizes that if a commander is interested in IO and its capabilities, then they will include it in their intent and concept of operations. To date, commanders have been left to sort out how they desire to implement IO capabilities due to a lack of clarity and depth from the available doctrine. Due to the lack of doctrine and the lack of information operations working group guidance, commanders tended to withhold capabilities and hold the right to execute IO only at the higher levels (Cox, 2006).

The CALL Initial Impressions Report (2005) identified a lack of understanding of the IO strategy, lack of command emphasis, and doctrinal and resource shortfalls as challenges with IO. Staffs were not intended to stovepipe the IO capabilities but to use the published processes to coordinate and synchronize information with the rest of the element of combat power to create an operational advantage (CALL, 2005). Two related challenges are the lack of command emphasis and the shortfalls of doctrine and resources. Commanders, early in operations, were generally unwilling to address IO because of their misunderstandings of "the efficiencies that IO integration brings to a complex operational environment" (p. iv). The study concluded that units must deploy "with the requisite skill sets, processes, and calibrated leadership that does not put them in a situation where they must re-task organize or operate inefficiently in a battle zone" (p. vii).

During development of FM 3-0, the Army noted the shift in focus for integrating IO capabilities and sought to meet the earlier demands to provide clearer doctrine with broader application. FM 3-0 (2008) introduced the Army Information Tasks, emphasizing the importance of conducting full spectrum operations and utilizing all elements of combat power, to include information, equally to achieve operational effects. In the manual the Army moves away from the integrating strategy of IO to the Army information tasks as a "comprehensive approach" to using information during full spectrum operations (Army, 2008, p. 7-2). The focus of the Army information tasks is on using the individual tasks — information engagement, command and control warfare, information protection, operations security, and military deception — to integrate information capabilities throughout the operations process and managed by the Chief of Staff, as means to shape the information variable of the operational environment. The manual states that commanders, "integrate information tasks into all operations and include them in the operations process from inception" (p. 7-2). The manual appears to identify the commander as responsible for successfully integrating information into battle command and integrating the tasks through the operations process (Army, 2008).

CALL reviewed observations, insights, and lessons from current operations in a Gap Analysis: Information Operations Report published in 2008. In the second paragraph of the executive summary section the report states that "doctrine within this field does not meet the requirements for the current force or future force" (p. viii). The report concluded that commands, at nearly every level, misunderstand IO as a force multiplier. Instead of treating IO as the horizontal synchronizing effort that it is, staffs tend to see it as a stovepiped effort. The report reinforces the fact that commanders and their staff are turning to lessons learned and best practices to understand how to using IO as an integrating strategy because current doctrine is insufficient for the current operating environments.

Cicalese (2009) reinforces the reports that commands misunderstand IO as an integrating function in his top ten myths article published in the Center of Army Lessons Learned library. In his third myth he discusses the misuse of terms and ignorance of our own doctrine. His discussion takes the reader back to the JP 3-13 (1998) identifying IO as an integrating strategy used to affect the adversary's decision making while protecting our own (Cicalese, 2009). Throughout the article he continually demonstrates the ability of "the IO model… be[ing] tailored to fit the mission based on the type of fight the unit has, where the unit is in that fight, and what type of headquarters the unit has" (Cicalese, 2009, p. 7). He notes that failure is not a result of the IO model but of "ignorance or inexperience born in the absence of available capabilities" (p. 7); therefore, units resort to using something they are more experienced with and have had success with in the past.

Murphy (2009) reinforces the conclusions of the Gap Analysis (2008) and Cicalese (2009) in an article published in the *IO Journal* in April 2009. He states, "a review of current and US government information-related lexicon and definitions points out a very obvious flaw: this stuff is confusing… and in some cases, self-defeating" (p. 18). Current doctrine does not provide commanders with the necessary 'how to' or clarity on how information-related capabilities fit within the mission requirements. Murphy (2009) defines a need to clean up the language and definitions to provide a clear understanding of the utility of the IO construct. Currently, when one reads the definition of IO they are drawn to one of the core capabilities of IO, making IO synonymous with PSYOP or with CNO, depending on the reader's specific area of expertise (Murphy, 2009 & Cicalese, 2009).

From the initial introduction of C3CM (1992) through publication of JP 3-13 (2006) the utilization of information has been viewed as a strategy for commanders to integrate information into military missions. Information are "facts, data or instruction[s] in any medium or form" and as "the meaning that a human assigns to data by means of the known conventions used in their representation" (DoD, 2009). IO is the military's strategy, "a prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multination objectives" (Army, 2008, p. 6-2). In this case, information operations are a "prudent idea" used to synchronize information by integrating IO capabilities within the mission plan through the operations process. In order to integrate capabilities, the Army, uses "integrating processes and continuing activities to synchronize operations during all operations process activities" (p. 5-20).

The Army initially chose to use the term information operations for two reasons. "First, it recognizes that information issues permeate the full range of operations from peace through global war. Second, this broader approach emphasizes the operational impact of information on knowledge-based operations at each and every echelon" (McConville, 1997). A common complaint related to this broad approach is that "IO is at once everything and it is nothing" (Armistead, 2004, p. 19).

The bottom line is that information can be used as an "effective tool for shaping the environment" throughout the spectrum of operations (Armistead, 2004). In order to successfully do this staffs take all aspects of information and combat capability into account in order to influence adversary decision-making and activities, while still providing protection of friendly information and information systems. As current operations are reviewed for strengths and weaknesses it is essential that leaders selectively apply the lessons learned to ensure that aspects of operations which are effective in one area are not universally applied to all operational areas.

Application and utilization of lessons learned should keep in mind the fact that the Army introduced the concept of Information Operations into its doctrine in 1996, specifically designed to "appl[y] an organizing architecture to the many activities focused on using information and information systems in support of military operations" (Hiemstra, 1999, p. 1). Through this process IO became an overarching concept used to discuss the actions used to attack command, control, computers, communication, and intelligence (C4I) through doctrinally identified capabilities (CALL, 2005).

Today, the concept of IO is still ambiguous and fluid, regardless of the numerous articles, comments, reviews, and studies identifying a need to clearly and concisely define this concept. Leaders and soldiers are taught to utilize weapons and weapon systems during military operations; however, IO is not a weapon, in the technical and traditional sense of the word but when leveraged, information provides a combat multiplier previously unavailable within the operational environment (Army, 2008). One continued reason for the confusion and lack of clarity in the doctrine is the continual changes to terminology and the theoretical application of the IO strategy from one publication to the next, generally with very few opportunities to truly test the revised theories in operations.

The introduction and evolution of these concepts has occurred over the last two decades to unify the once separate successes of information capabilities into an integrated strategy, utilizing information as a force multiplier without over extending already sparse resources. Separating these capabilities out among the staff increases the operational requirements on already over tasked and undermanned sections of the command and assumes that the operations process is sufficient to integrate all aspects of information into the overall operation without assigning personality responsibility to anyone. It appears that the Army is disregarding the need for an integrating strategy that creates a unity of effort for information capabilities. The construct does emphasize a need to utilize the breadth of knowledge required to successfully employ these very complex capabilities, but fails to bring the expertise together in a single functional or integrating cell.

Commanders and their staffs continue to misunderstand IO as a combat multiplier at every level, continuing to treat it as an under resourced and stovepiped staff function. When in fact, it should be a strategy used to horizontally synchronize efforts across the staff. Some of the continuing problems come into play when trying to delineate a clear relationship between IO and the associated capabilities (CALL, 2008). However, the linkage is in the definition of information, realizing that manipulation, dissemination, and/or collection of facts,

data, and instructions across available mediums must have meaning to the intended audiences. IO is used to integrate the relevant capabilities with one another and to ensure those capabilities are synchronized across the staff for coordination with the entire operation to successfully influence the behaviors and attitudes of the intended audience.

Ultimately, the introduction of the five information tasks appears to take the Army back to the individual application of capabilities which was used prior to 1979, when C3CM was first introduced as an integrating strategy. The subsequent changes, adjustments, addition and subtraction of terminology and lack of clarification on the evolving theory have served to further complicate an already complex theory proven to provide a very valuable strategy to commanders. However, the introduction of the Army information tasks neither appears to clarify the 20 plus years of theory or the original idea of providing an integrating strategy for applying information as a force multiplier/element of combat power.

*Major Nicoline Jaramillo is an IO Officer for 4th Brigade, 1st Armor Division out of Fort Bliss, TX. She previously worked as an Information Engagement planner for USAIOP, a year conducting research and assisting with the doctrine process with the Combined Arms Doctrine Directorate, and three years as an IO plans and targeting officer for 8th US Army. MAJ Jaramillo received a BS degree in Psychology from the University of Idaho, an MS degree in Industrial Organizational Psychology from Capella University, and an MBA in Management and Leadership from Webster University, where she did research on the applications and utility of Information Operations and her final project was a historical analysis of Army IO.*

## REFERENCES


Armistead, L. (2004). Information operations: Warfare and the hard reality of soft power. A textbook produced in conjunction with the Joint Forces Staff College and the National Security Agency. Washington, DC: Brasseys, Inc.

Army, Deparment of (1992). *Army Regulation 525-20, Command and Control Countermeasures (C2CM)*. Washington, DC: Department of the Army.

Army, Deparment of (1996). *FM 3-13 Information Operations.* Fort Leavenworth: Department of Defense.

Army, Deparment of (2003). *FM 3-13 Information Operations.* Fort Leavenworth: Department of Defense.

Army, Department of (2008). *FM 3-0 Operations.* Fort Leavenworth: Department of Defense.

Baker, R. O. (2006) . The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations. *Military Review,* p. 13-32.

Berkowitz, B. (2003). The new face of war: How war will be fought in the 21st century. New York, NY: Free Press.

CALL (2008). Report Gap Analysis: Information Operations. *Center for Army Lessons Learned*. Retrieved June 1, 2008 from https://call.army.mil. (This is a password protected site and the document is classified For Official Use Only).

CALL (2005). *Information Operations. Initial Impressions Report, No. 05-3*. Center for Army Lessons Learned. Retrieved October 3, 2005 from http://call.army.mil.

Cicalese, C. (2009). NFTF: Information Operations Top Ten Myths. *Center for Army Lessons Learned*. Retrieved April 22, 2009 from https://call2.army.mil/toc.aspx?document=4837 (This is a password protected site and the document is classified For Official Use Only).

Cox, J. L. (2006). *Information Operations in Operations Enduring Freedom and Iraqi Freedom — What went wrong?* Retrieved March 1, 2009 from http://www.fas.org/irp/eprint/cox.pdf.

Denzin, N. K. and Lincoln, Y. S. (1994). Handbook of qualitative research. Thousand Oaks, CA: Sage Publications, Inc.

Department of Defense, (2009). DoD Definitions: Information. Retrieved April 15, 2009 from http://www.dtic.mil/doctrine/jel/doddict/data/i/02633.html

Emery, N. (2004). Information Operations in Iraq. *Military Review,* p. 11-14.

Glenister, C. A. (2001). Information Operations in the IBCT. *Military Review*, p. 59-62

Hawkins, C. F. (1997). *Coming to Grips with Information Warfare: A Western Perspective*. Beijing Special Lecture, March 1997 at China Defense Science and Technology Information Center. Retrieved April 12, 2009 from http://www.herolibrary.org/iwa4web.htm.

Herndon, R. B, Creighton, J. L. & Bello, L. J. (2004). Effects-based Operations in Afghanistan: The CJTF-180 Method of Orchestrating Effects to Achieve Objectives. *Field Artillery*, p. 26-30. Retrieved March 15, 2009 from https://www.au.af.mil/au/awc/awcgate/army/ebo_afghan.pdf.

Hiemstra, M. A. (1999). Task Force Eagle: Information Operations. CALL Newsletter, 99(2), p. 1-81. Retrieved October 11, 2005 from http://call.army.mil.

Leedy, P. D. and Ormrod, J. E. (2005). Qualitative research. Practical Research: Planning and Design, 8th Ed. (p. 133-160). Upper Saddle River, NJ: Pearson, Merrill-Prentice Hall.

Macke, R. C. (1993). Command and Control Warfare. *Chairman of the Joint Chiefs of Staff Memorandum of Policy No. 30.* Retrieved April 12, 2009 from www.dod.gov/pubs/foi/reading_room/732.pdf.

McCausland, J. D. (2000). Information operations primer. US Army War College. Retrieved October 25, 2005 from http://call.us.army.mil.

McConville, J. E. (1997). US Army Information Operations: Concepts and execution. Retrieved November 11, 2005 from http://www.fas.org/irp/agency/army/tradoc/usaic/mipb/1997-1/mcconv1.htm.

Murphy, D. (2009). Talking the Talk: Why Warfighters Don't Understand. *IO Journal,* p. 17-39. Retrieved May 1, 2009 from https://www.carlisle.army.mil/DIME/documents/IP%204-09%20-%20Talking%20the%20Talk.pdf.

Pace, P. (2008). *Joint Operations*. Retrieved March 1, 2008 from http://www.dtic.mil/doctrine/jel/new_pubs/**jp3_0**.pdf.

Povel, E. (2000). The Kosovo crisis and the media: Reflections by a NATO official. *NATO Office of Information and Press* . Munich, Netherlands: NATO.

Romanych, M. J. & Krumm, K. (2004). Tactical information operations in Kosovo. *Military Review* , 56-61.

Rumsfeld, D. H. (2003). *Information Operations Roadmap.* Retrieved March, 12, 2009 from www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

Shelton, H. H. (1998). Joint Publication 3-13: Joint Doctrine for Information Operations. Retrieved October 8, 2005 from www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

Shelton, H. H. (2006). Joint Publication 3-13: Joint Doctrine for Information Operations. Retrieved October 8, 2005 from https://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

Smith, C. F. (1983). Command, Control, and Communications Countermeasures (C3CM). *Army Communicator*, p. 49-53. Retrieved Arpil 1, 2009 from www.gordon.army.mil/ocos/ac/articles/1983/c3cm.pdf.

Thomas, T. L. (2000). Kosovo and the current myth of information superiority. *Parameters* , 13-29.

Trent, S. and Doty, J. L. (2005). Marketing: An overlooked aspect of information operations. The US Army Professional Writing Collection. Retrieved November 21, 2005 from http://www.army.mil/professionalwriting/volumes/volume3/october_2005/10_05_1.html.

Wallace, W. S. (2008). FM 3-0 Operations: The Army's Blueprint. *Military Review,* p. 2-7.

Wass de Czege, H. (2008). Rethinking "IO:" Complex operations in the Information Age. Small Wars Journal, July 4, 2008. Retrieved July 7, 2008 from http://smallwarsjournal.com/mag/2008/07/rethinking-io-complex-operatio.php

Wikipedia (2005). Military doctrine. Wikipedia: The free encyclopedia. Retrieved December 11, 2005 from http://en.wikipedia.org/wiki/Military_doctrine.

Wolfowitz, P. (2001). Information Operations. *Department of Defense Directive #3600.1*.

Wright, R. H. (2001). Information Operations: Doctrine, Tactics, Techniques and Procedures. *Military Review*, p. 30-32.

# Recommendations Regarding the Information Component of Power for the 2009 National Security Strategy

**By LTC Simon R. Goerger, Ph.D.**

"The national security and economic health of the United States depend on the security, stability, and integrity of our Nation's cyberspace, both in the public and private sectors." –John Brennan, Assistant to the President for Counterterrorism and Homeland Security. (1)

## Introduction

In promoting and protecting the interests of the United States, the President and his staff face numerous issues. To address these issues, the President has at his disposal a variety of instruments spanning the kinetic spectrum. In this era marked by the rapid evolution of cyberspace, the information component of national power is an emerging area into which influential international instruments fall. This paper describes the information component of power within the context of national power and outlines how the United States should develop and employ this component as a means of executing the *2009 National Security Strategy* to attain its national security objectives.

## National Power

National power consists of four primary elements — diplomatic, information, military and economic (DIME) (2). The information element, or component, of national power acts as a force multiplier for the other three elements of national power. First, the diplomatic power uses information power to enhance the capabilities to spread the nation's strategic message. Second, military power uses information power to inform the command and deny assets to the enemy during the use of military power. Finally, the use of information power to maintain the data and products behind the economic engine of our national and global economies provides a daily reminder of its ability to be a force multiplier.

One can categorize elements of national power in numerous ways: absolute versus relative; concrete versus perceptual; expandable versus limited; potential versus latent; or soft versus hard (3). For the purposes of this paper, the soft versus hard power construct will be used to elaborate on the functionality of information power as it relates to the kinetic spectrum of options. "Soft power… is the ability to get desired outcomes because others want what you want," (4) while "hard power is the ability to get others to do what they otherwise would not do through threats or rewards." (5) Information power is one unique component of national power that can be soft or hard and thus resides along the kinetic spectrum of operational alternatives. One categorizes information power based on its "ways" and "ends". As a means of informing one's allies of our national interests and capabilities, it is a means of soft power. However, a commander can use information power in kinetic operations against his adversaries, thus employing it as a means of hard power. It provides the commander with the strategic advantages of understanding his enemies better and affording more time to maneuver hiss assets into position to coerce or defeat his enemies.

This duality of information power is a characteristic of what Joseph Nye defines as *smart power (6)*. By projecting soft power to facilitate coordination with allies and blunt hard power to control state and non-state activities it proves to be a flexible tool effectively used by skilled leaders.

## Information Power

The *information component of power* is "the relative ability to operate in and exploit… the combination of Connectivity, Content, and Cognition operating within a complex human, political and technological context to generate strategic advantage." (7) Man has conducted information operations for centuries. However, with the invention of the telegraph, man opened the door to the cyberspace domain as he began to pass information using electrons (8). The domain of cyberspace is the newest of the five domains in which the United States traditionally conducts operations (i.e. land, sea, air, space and cyberspace). To characterize cyberspace more definitively Dr. Dan Kuehl defines and describes cyberspace using the three major facets: connectivity, content and cognition ("3 C's").(9)

Similar to those described by Dr. Kuehl as the "3 C's, **Figure 1** summarizes the three dimensions of the information environment as outlined in *Joint Publication 3-13, Information Operations*.

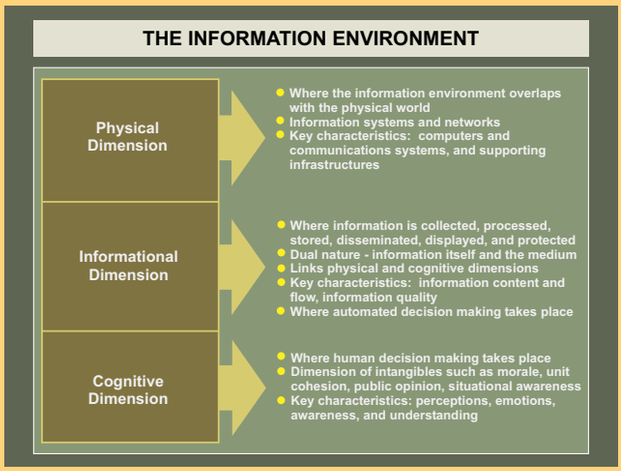



*Figure 1: Information Environment (From Joint Publication 3-13) (10)*

## Information Environment: the "3 C's"

*Connectivity* is the basic means or infrastructures that allow one to deliver information. In the more traditional domains of land and sea, the infrastructure for information delivery includes things such as printing plants, bulletin boards, sound systems, town squares, and other systems or structures that provide a means to process, transport, or display information. In cyberspace, the infrastructure or means involves electronic communications mechanisms and structures. Connectivity consists of physical components such as the networks of wires, routers, servers and workstations as well as the human operator and his cognitive capacity. *Content* includes the products that exist in and moves through cyberspace. It is words, images and databases. At the lowest level, it is the "1's" and "0's" and one day will be the fractions of electronic impulses that represent information and data. Cyberspace can present content in numerous ways (e.g., written word, verbal communications, visual displays, and tactile feedback).*Cognitive* refers to the ability of a human to take content and process it into knowledge and understanding. It provides the ability to influence the recipient. How one presents information has an impact on the ability of the consumer to process and interpret it. More than information itself, it is the way one packages and presents information that allows for consumer consumption in a manner that allows one to achieve one's interests.

For example, a listing of books and prices on a webpage may enable a consumer to find and purchase a book. However, a search engine that locates a subset of books and displays book titles, authors, prices, covers, descriptions of content, and a series of reviews helps ensure one is purchasing the book one truly desires.

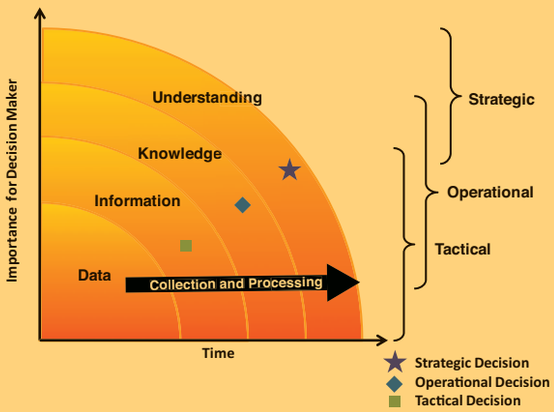



*Figure 2: Data to Understanding and Decisions Paradigm (Based on Goerger and MCDP 6) (11)*

**Figure 2** illustrates the method to take basic data residing in the information environment, process it into information and pass it on to decision makers for cognitive consumption. Once information reaches the human component of the environment, consumers use it to create knowledge and understanding. Leaders of industry and government use this knowledge and understanding to conduct business and execute policy. The figure also illuminates the impact of network systems that allow for the processing of massive amounts of data in a timelier manner to produce and distribute meaningful products to the decision maker. It also indicates the escalating importance to a decision maker on information, knowledge and understanding for making decisions at each successive level of command.

The cyber component of the information environment facilitates the ability to enhance the volume and speed at which systems gather data and analysts produce information for leaders. This is one of the keys to success in the global economy of the 21st Century. Individuals and nations who harness and utilize cyberspace gain an ability to create knowledge and understanding more rapidly. This allows them to more effectively influence other actors and achieve their strategic interests. This is the goal of information power.

## Information Power in the Department of Defense Framework

To evolve the concept of information power, a doctrinal example of how the Department of Defense (DoD) provides a component of the nation's information power is illustrated in Enclosure 1, **Figure 3.** This provides a glimpse into the complex architecture and management required to harness this power successfully. **Figure 3** demonstrates the paradigm where national information power is the superset in which DoD information operations (IO), information warfare (IW) and command and control warfare (C2W) reside.(12) C2W is comprised of five pillars that together provide the commander the tools required to conduct IW. C2W's five pillars are destruction, deception, psychological operations, operations security and electronic warfare (13).


*Figure 3. Paradigm Kuehl (From Kuehl, Joint Information Warfare 1997) (14)*

Information warfare is the military component of information operations. It is the offensive and defensive actions a commander can use to control or exploit the environment. (15) Information Warfare includes C2W capabilities and other related activities such as Civil Affairs, computer network attacks and Public Affairs. When and where IO includes IW, it also consists of operations from other government agencies designed to protect as well as control or exploit the global information environment. As the superset, national information power is comprised of the nation's commercial and military IO capabilities that enable the exploitation of the global information environment from a strategic perspective (16). **Figure 4** depicts the nested nature of Information Warfare as a subset of Information Operations. It also shows how Information Operations span the political/diplomatic, information, military and economic infrastructures. This provides context for how information operations works as a force multiplier for all four national power elements, DIME. It also provides linkage between the three objectives categories and three decisions levels (tactics, operations, strategic) found in **Figure 2**.

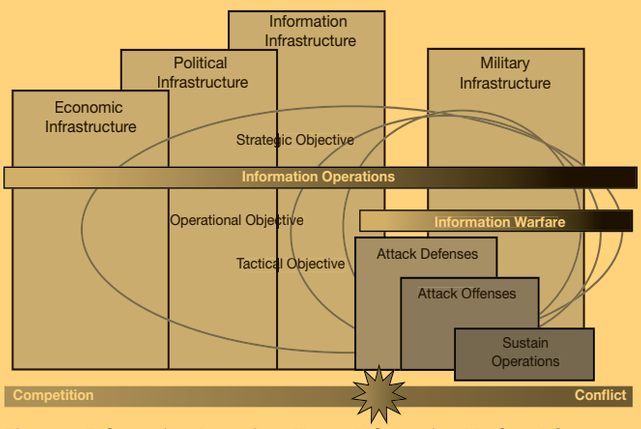



*Figure 4: Information Operations Versus Information Warfare Spheres (From Armistead 2004) (17)*

## Measuring Information Power

The ability to measure information power as a force multiplier and to identify its effective uses differs as compared to the ability to measure diplomacy, military or economic powers (18). Leaders often see within hours or days the impacts of information power on national interests due in part to the speed at which content passes through the information environment to reach large virtual audiences through cyberspace. Although well-crafted products can generate desired responses in some cultures, they can readily create undesirable and unintended responses in others based on the packaging of the message that can continue to reside in cyberspace causing old and new wounds to fester. For example, messages enumerating the members of the "Axis of Evil" may identify our friends and allies today but inhibit future efforts to gain positive relations with these states. Additionally, images such as those circulated on the Internet, can easily be modified or used to create a devastating message from which it is difficult to recover (e.g., Tuvia Grossman image in the *New York Times*, 2000) (19).

Given the short-term delivery, ability to promulgate, and potential long-term effects of information power, one must measure multiple qualitative and quantitative aspects of this power to understand its current and relative effectiveness. One viable means is to assess a nation's information power capabilities and effectiveness based on the "3 C's". Connectivity lends itself nicely to the use of quantitative measures while cognition can be primarily assessed using qualitative measures. One can assess content using both qualitative and quantitative measures. Connectivity measures should assess at least four factors. The first measure is the percentage of cyberspace penetration in the country. For the United States, this value as of June 2008 is approximately 72.5 percent (20).

**Table 1** provides Internet usage statistics and population numbers for the United States, North America, the world minus North America and the entire world. The numbers indicate the United States and North America are well ahead of the majority of the world in the use of the Internet. The United States and North America have over 72.5 percent and 73.6 percent, respectively, of their populations using the Internet. The remainder of the world averages 19.2 percent Internet penetration of its population. To determine the maximum percentage of population penetration, one considers it in context of the national adult literacy rate. As a nation evolves from a preponderance of the population being digital immigrants to the majority of the nation being digital natives, the national cyberspace user internet penetration rate should reach values similar to the adult literacy rate (21).

Second, one should measure the percentage of the nation covered by internet access. A possible goal value of approximately 95 percent of the nation's land mass being accessible to the internet via wire or wireless systems is one example. The third measure should be the percentage of user capacity of the

| Internet Usage and Population Statistics for North America | | | | | | |
|---|---|---|---|---|---|---|
| | Population ( 2008 Est. ) | % Pop. N. A. | Internet Usage, Latest Data | % Population (Penetration) | % Users N. A. | Use Growth ( 2000-2008 ) |
| United States | 303,824,646 | 90.10% | 220,141,969 | 72.50% | 88.70% | 130.90% |
| Total for North America | 337,167,248 | 100.00% | 248,241,969 | 73.60% | 100.00% | 129.60% |
| Rest of the world | 6,338,953,040 | 94.90% | 1,215,390,392 | 19.20% | 83.00% | 380.60% |
| World Total | 6,676,120,288 | 100.00% | 1,463,632,361 | 21.90% | 100.00% | 305.50% |

*Table 1: Internet Users and Populations Statistics for United States and the World - 2008 (Based on Internet Usage and Population in North America. (22)*

network systems and how it compares to industry standards for available bandwidth per user. It measures the ability of the nation to maintain interoperability within the domestic network. The final measure is the percentage of external accessible bandwidth per user. This measures the users' ability to access content and interact with users outside the boundaries of the nation's domestic cyberspace.

Measuring content provides a means of assessing use of cyberspace and one can relate the measure to the quantity and quality of the products produced. The volume of new materials can be measured by the monitoring the amount of traffic generated and consumed by the nation's users. I propose analysts create a "products per user" score by dividing the number of products produced by the number of users in the nation. Analysts use "products per user" scores to generate relative ranking to other nations. The assumption is the higher the number of products generated per user, the more familiar and comfortable the users are with operating in cyberspace. To assess the impact of information power on diplomacy, military and economic power, the government can measure the percentage of new products developed in each domain. Other categories to add to this list of DIME domains would include entertainment (e.g., music, movies, and games) and personal communications (e.g., personal emails and MySpace postings).

Finally, one must assess the quality of the products produced. These are subjective measures based on a sample of products from each domain (e.g., diplomatic power, entertainment, and personal communications) assessed by teams of subject matter experts using Lickert scales (23).

Measures of performance for cognition are qualitative in nature and should assess the ability of users to access data, produce information, assimilate knowledge and obtain understanding. The government can obtain qualitative performance scores through standardized testing such the Scholastic Aptitude Test for high school students or the Armed Services Vocational Aptitude Battery. I propose the Department of Education and DoD develop a new standardized Cyber Aptitude Test and administer it at the start or completion of professional schooling (e.g., prior to completion of an undergraduate or graduate program, profession military development course, executive level or capstone course). These testing venues would provide a pool of representative participants from which the government to assess the ability of individuals who use the information environment, *cyberspace professionals*, to execute their professional requirements. One can assess industry performance via testing of cyberspace professionals and utilizing professional certification program statistics.

## Challenges

Many challenges exist in the use of information power and the maintenance and development of the information environment. This is especially evident in cyberspace where due to its borderless nature and global reach its effects are rarely localized. Below I discuss the challenges regarding infrastructure, organizations and people, information validity and norms for use and policing.

The information environment infrastructure has developed quickly and in an ad hoc fashion over the last three decades. Compounded by the iterative development of hardware and software to meet the demands of users, many components of the system are non-interoperable or close to maximum utilization. Industry needs to replace many of the outdated systems. Also, much of the backbone architecture (e.g., fiber cables, satellite systems, and routers), under the guidance of government regulations and treaties, needs reengineering to provide more resiliency and robustness in the system. Furthermore, additional system security measures are required to protect the validity and integrity of the data.

Interagency operations and limited doctrine describing the purpose and use of information power creates interoperability issues between organizations and inhibits our ability to maximize national use of the information environment. A lack of understanding by digital immigrants (24) regarding the strengths and weaknesses of the cyber component of the information environment cripples our ability to identify appropriate uses and emplace appropriate infrastructure for future requirements. The adverse effect of digital immigrants is waning as digital natives (25) rise to positions of power and digital immigrants become more comfortable with their new cyber environment. Further education is required to ensure digital immigrants and digital natives have more than a cursory understanding of the dynamic cyberspace.

The borderless nature of cyberspace presents issues with policing the use of the environment. Attempting to identi-

fy the true source of system abuses or malicious actions is difficult at best and compounded by the lack of codified international norms for dealing with violators. No formal internationally recognized collection of state actors exists who can provide these norms and outline appropriate remedies for wrongs committed against state and non-state actors. Dealing with non-state actors that reside in or transgress multiple states compounds the issue.

## Recommendations Regarding Information Power for the National Security Strategy

The nation's information strategy, within the context of the National Security Strategy, must address the strengths and weaknesses of information power and how our nation will use the information component of power as a force multiplier. As we have seen, the information component of power is an integral element used in our daily lives in the conduct of diplomacy, military operations, business and entertainment. We can effectively use it; likewise, it can effectively be used against us. To use national information power effectively to promote and defend our national interests, we must learn to harness and utilize the information environment. Our information power development strategy must address capabilities and requirements of the "3 C's" of the information environment. The use of information power requires the defense of the connectivity infrastructure to maintain current capabilities. It also necessitates continued development of the infrastructure to increase resilience, ensure availability, and maintain security and integrity of the data.

National content requires a coordinated effort between industry and government to promote good news stories and national values while protecting the validity of data and credibility on products posted to cyberspace. Protecting the validity of data is a component of information assurance. Insuring the credibility of products requires professionalism of product developers and critical peer review prior to the posting of the products. Once posted to cyberspace, the products will take on a life of their own and the ability to contain the adverse effects of inaccurate or poor products is limited.

To build cognition requires a set of skills that the education system can teach using appropriate methodologies and individuals can perfect through use. Requiring courses in critical and logical thought processes (e.g., math, theology, and philosophy) provides users with the fundamental foundation to assess information in a critical manner and process it for knowledge and understanding. Further research is ongoing and more is required to determine how to build or enhance cognition. None of these is a short-term endeavor. They are long-term, generational, approaches to improving our use of information operations in cyberspace. To understand properly the strengths and weaknesses of information power, we must develop the battlefield by positioning resources and providing enhanced skill sets for our citizens. This will allow practitioners of cyberspace to adapt to the changing information environment.

As a force multiplier, information power requires special emphasis. To this end, the National Security Council should have an Information Operations Czar to communicate the President's information strategy, identify and allocated available resources, and deconflict issues between departments. One can find additional key roles and responsibilities of information strategy implementers in **Table 2**.

Table 2. Key Roles and Responsib ilities of U.S. Information Strategy

| Key Roles and Responsibilities of Information Strategy | |
|---|---|
| President of the United States | · Provide the nation with an information operations strategic vision to prioritize objectives and guide the efforts of US resource managers<br>· Establish an Information Operations Czar as a member of the National Security Council<br>· Authorize the Information Operations Czar to deconflict information operations issues between other government agencies |
| Government Organizations | · Congress: Develop/assess/pass laws for the proper use of domestic cyberspace<br>· Congress: Review/approve international cyberspace treaties based on international norms for the proper use of cyberspace<br>· Congress: Regulate development and appropriate use of the domestic information environment<br>· Congress: Provide research funding to education institutions for educating future developers and managers of the information environment<br>· Congress: Provide research funding to education institutions for the fundamental development of new technologies to assist in enhance the capabilities and reliance of the information environment<br>· Congress: Provide DoD funding to train, equip and lead digital warriors and staffs<br>· Information Operations Czar: communicate the President's information strategy, identify and allocated available resources, and deconflict issues between departments<br>· Department of State: Negotiate international cyberspace treaties based on international norms for the proper use of cyberspace; develop plan for International Cyberspace Coalition to identify/develop norms for the use and policing of cyberspace<br>· Department of Homeland Security: Identify key cyberspace infrastructure components, assess their current status on an annual bases, and develop a five year and ten year plan to maintain and enhance the nations cyberspace infrastructure<br>· NSA: Monitor cyberspace for in appropriate activities, track cyber crimes, coordinate with appropriate agencies to police inappropriate cyberspace activities<br>· CIA: Police international cyberspace issues<br>· FBI: Police domestic cyberspace issues<br>· Treasury: Track and policy cyberspace transactions<br>· Education Department: Develop a national Cyberspace Aptitude Test for high school seniors, DoD personnel, and civil servants; assess industry efforts in professional cyberspace certifications for appropriate inclusion (e.g. Certified Information Systems Security Professional (CISSP) and Certified Modeling & Simulation Professional (CMSP) |
| Military | · Prepare to coordinate and conduct Information Operations<br>· Train, equip and lead digital warriors and staffs to collect data and produce intelligence documents to help in the planning for and possible execution of kinetic or peacekeeping operations |
| International Partners | · Track cyberspace transactions and inform appropriate countries of any illegal activities that cross international boarders<br>· Develop an international organization to establish formal norms for appropriate use of cyberspace<br>· Develop an international organization to police cyberspace for violation extended across nation state boarders |
| Industry | · Maintain current information environment infrastructure, conductivity<br>· Develop enhanced infrastructure to meet new demands, protect commerce and consumer confidence in the validity and security of data and information products<br>· Develop a national Cyberspace Aptitude Test for business professionals; assess industry efforts in professional cyberspace certifications for appropriate inclusion (e.g. Certified Information Systems Security Professional (CISSP) and Certified Modeling & Simulation Professional (CMSP) |

*Table 2: Key Roles and Responsibilities of U.S. Information Strategy*

## Conclusion

Information power is a force multiplier that plays an essential role in U.S. National Security Strategy. As an element of smart power, it operates in the realm of the information environment to support the diplomatic, military and economic power domains. An emergent and massive component of the information environment is cyberspace. Cyberspace is subdivided into the "3 C's": connectivity, content and cognition. America's information strategy must measure, assess and address the shortcomings of information power through the "3 C's". One can measure and assess a nation's information power by addressing the qualitative and quantitative factors of the "3 C's". This paper defined the information component of power and outlined how the United States should strategically develop and employ this component of DIME as a means of executing the *2009 U.S. National Security Strategy* to attain U.S. national security objectives.

*Simon R. Goerger, Ph.D., is a Lieutenant Colonel in the U.S. Army and a student at the National War College, Fort McNair,*

*Washington, D.C., (202) 685-3684. His follow-on assignment is with the Office of the Secretary of Defense - Personnel and Readiness, Readiness Programming & Assessment, Washington, D.C., (703) 693-5584. He recently served as the an Assistant Professor and the Director of the Operations Research Center of Excellence in the Department of Systems Engineering at the United States Military Academy, West Point, New York before deploying to serve as the Joint Multinational Networks Division Chief, Coalition Forces Land Combatant Command/U.S. Army Central Command, Kuwait. He earned his Bachelor of Science from the United States Military Academy in 1988 and his Masters in Computer Science and Doctorate in Modeling and Simulations from the Naval Postgraduate School, Monterey, CA in 1998 and 2004, respectively. His research interests include systems modeling, combat modeling and simulations, agent based modeling, human factors, and training in virtual environments. LTC Goerger has served as an infantry officer with the 6th Infantry Division in Alaska and Sinai, Egypt, as a cavalry officer with the 2d Armored Cavalry Regiment at Fort Polk, LA and Port-a-Prince, Haiti, and as a software engineer for COMBATXXI, the US Army's future brigade and below analytical model for the 21st century.*

## ENDNOTES

1) J.D. Kathuria "Obama taps local expert Melissa Hathaway for key cyber role," *ExecutiveBiz*, LLC, February 10, 2009, http://blog.executivebiz.com/tag/john-brennan (accessed April 16, 2009).
2) Joint Chiefs of Staff. *Joint Publication 3-13, Information Operations*. Joint Publication, Washington, D.C.: Joint Chiefs of Staff, February 13, 2006.
3) Categories are extracted from Deibel, Terry L. *Foreign Affairs Strategy; Logic for American Statecraft*. New York, NY: Cambridge University Press, 2007.
4) Keohane, Robert O., and Jr. Joseph S. Nye. "Power and Interdependence in the Information Age." *Foreign Affairs*, September/October 1998: 86.
5) Ibid.
6) Nye, Joseph S. *The Powers to Lead*. Oxford, NY: Oxford University Press, 2008.
7) Daniel T. Kuehl, "The Information Revolution and the Transformation of Warfare." Chap. 29 in *The History of Information Security: A Comprehensive Handbook*, edited by Karl de Leeuw and Jan Bergstra, 821-832. Amsterdam, The Netherlands: Elsevier B.V., 2007. *Joint Publication 3-13, Information Operations* states: "the information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is made up of three interrelated dimensions: physical, informational, and cognitive."
8) "Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures." From Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem." *Airforce Symposium 2008: Cyberspace*. Air University (AU) Maxwell AFB: National Defense University, Information Resources Management College, July 15-17 2008.
9) Daniel T. Kuehl, "The Information Revolution and the Transformation of Warfare." Chap. 29.
10) *Joint Publication 3-13, Information Operations* breaks down information environment into three similar categories (see Figure 1). Joint Chiefs of Staff. *Joint Publication 3-13, Information Operations, 1*-2.
11) This diagram is based on discussions in May and June of 2008 amongst COL Michael Yarmie, LTC Scot Ransbottom, LTC A.J. Danahuer, LTC Mike Bartlett and LTC Simon R. Goerger of the G6, U.S. Army Central Command, Camp Arifjan, Kuwait. It is visualization and extension of the concepts of information hierarchy and image theory as outlined in MCDP 6, *Command and Control* (Washington DC, Department of the Navy, 1996), pp. 66-76.
12) Figure 3 does not depict the commercial or civilian information operations component of national information power.
13) Edwin L. Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power (Issues in Twenty-First Century Warfare)*. 1st. Dulles, VA: Brassey's Inc, 2004. 22.
14) Daniel T. Kuehl, *Joint Information Warfare*.
15) Figures 3 and 4 illustrate this fact.
16) Edwin L. Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power (Issues in Twenty-First Century Warfare)* page 16-20 and Daniel T. Kuehl, *Joint Information Warfare*. Washington, D.C.: National Defense University Strategic Forum, 1997.
17) Edwin L. Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power (Issues in Twenty-First Century Warfare)*, 20.
18) There are several conventional metrics used to measure diplomatic progress, military effectiveness, and economic health. On the other hand, metrics for measuring information power are newer and less-well defined. In addition, the prevalence of the information element of power and the means by which it intertwines with the other elements challenge the applicability of the conventional metrics. For example, traditional metrics for military effectiveness generally apply to more kinetic operations (e.g., loss exchange ratio) vice peacekeeping (winning the hearts and minds). One could measure the number of leaflets dropped over an area within a week but that does not reflect whether the desired effect achieved by the leaflets. There is a great deal of research ongoing in this area today. The metrics I propose in the main body of the paper will provide pointers indicating the current state of the information environment in our country and other nations and how help provide suggestion on where to cultivate information power for our national interests.
19) On 30 September 2000, the New York Times ran a photograph on page A6 with text describing an Arab man beaten by an Israeli police officer at Jerusalem's Temple Mount. In reality, the image was of Mr. Tuvia Grossman, the bloodied young man, a Jewish student from Chicago seeking protection from an Arab mob that had beaten and stabbed him. The Israeli police officer was coming to Grossman's aid. Additionally, the incident occurred near the Western Wall in an Arab neighborhood of Jerusalem, not the Temple Mount. From Grossman, Tuvia. Tuvia Grossman tells in his own words how Palestinians tried to lynch him, and how this event highlights the power of the media to influence public opinion. November 5, 2000. http://www.aish.com/jewishissues/israeldiary/Victim_of_the_Media_War.asp (accessed December 3, 2008).
20) Miniwatts Marketing Group. Internet Usage and Population in North America. June 2008. http://www.internetworldstats.com/stats14.htm (accessed November 14, 2008).
21) The adult literacy rate for the United States in 2008 was approximately 99%. From Central Intelligence Agency (CIA). Field Listing - Literacy. November 20, 2008. https://www.cia.gov/library/publications/the-world-factbook/fields/2103.html (accessed December 3, 2008).
22) Data extracted from Miniwatts Marketing Group. Internet Usage and Population in North America. June 2008. http://www.internetworldstats.com/stats14.htm (accessed November 14, 2008).
23) Analysts often use Lickert scales to assess relative quality of products. Scales can be of varying length but are normally odd in number (e.g. five, seven) to provide graders with the ability to distinguish between acceptable and unacceptable assessments. The questions could be similar to those used to assess/analyze the quality and effectiveness of media products produces. Once the questions are developed, assessment developers properly grounded the scales to provide adequate understanding to graders (subject matter experts)on what each value would indicate.
24) "Those of us who were not born into the digital world but have, at some later point in our lives, become fascinated by and adopted many or most aspects of the new technology are… Digital Immigrants." From Marc Prensky, "Digital Natives, Digital Immigrants." On the Horizon, Bradford, UK: MCB University Press 9, no. 5, October 2001, 1-3, http://www.emeraldinsight.com/Insight/viewPDF.jsp?contentType=Article&Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/2740090501.pdf (accessed November 13, 2008).
25) Digital Natives "have spent their entire lives surrounded by and using computers, videogames, digital music players, video cams, cell phones, and all the other toys and tools of the digital age. Computer games, email, the Internet, cell phones and instant messaging are integral parts of their lives. [As a result, they] think and process information fundamentally differently from" Digital Immigrants. Marc Prensky, "Digital Natives, Digital Immigrants," 1.

# Lessons to be Learned from a Recent Network Infrastructure Attack

By L. Scott Johnson and Toni Whyte

Early on Thursday April 9, 2009, a person or persons unknown deliberately severed AT&T-owned fiber-optic cables at multiple locations in the San Francisco Bay Area, near Silicon Valley. Landline and wireless communications were lost in southern Santa Clara County and parts of Santa Cruz and San Benito Counties, an area spanning about 100 miles. Internet access was lost, banks and businesses shut down, hospital operations were disrupted, and the 911 emergency communications network went dead in the affected areas. After about 12 hours, some service had been restored, and complete service was resumed within about 24 hours.

Public reaction to this event was mixed. Some commentators compared it to a terrorist attack on the US communications infrastructure — that is, an Information Operations attack. Others dismissed it as being little more significant than the accidental cable cuts that occur from time to time ("backhoe incidents").

After a few weeks, discussion of the incident largely disappeared from news outlets and online sites.

Given the extent to which targeted IO attacks on US network infrastructures are highlighted as critical threats to national security, it is instructive to examine this real-world example of such an attack. In this paper, we review the sequence of events and consequences, as reflected in press reporting and online discussions, and we examine the implications and lessons that may be learned.

## The Attacks

Some time before 1:25 a.m. Thursday April 9, 2009, someone lifted a heavy manhole cover on a cable vault near Monterey Highway in San Jose, CA, climbed down 8 to 10 feet and cut four fiber-optic cables owned by AT&T. One cable contained 360 fibers and the other three had 48 fibers each (1). This attack created most of the service disruption. At least one of the cables was leased by Verizon, which is the sole provider of landline services in the southern Santa Clara County area, thus about 52,200 households in those cities, along with customers in Santa Cruz County, lost service. Wireless service was lost also, owing to the loss of cable connectivity to cellphone towers (2, 3). Later, two more AT&T cables on Hayes Avenue in south San Jose were cut.

Between 4 a.m. and 5 a.m., four more fiber-optic cables were cut at two adjacent locations along Old County Road in San Carlos, which is about 40 miles north of San Jose. Two of these cables belonged to AT&T and one was owned by Sprint; it served customers of Sprint's wireline IP data service as well as some cellular towers. Sprint was able to restore at least some service after a couple of hours by rerouting traffic (some reports said Sprint customers were not seriously affected) (4,5). According to local officials, this was the largest phone outage in the area in recent history (6).

The sabotage crippled operations at hospitals, businesses, banks, and police and fire departments. The emergency 911 service was lost, police access to central databases was lost, computerized medical records became inaccessible, fire and burglar alarms were disconnected, and monitoring of critical utilities was interrupted (7). ATMs were inaccessible, and credit and debit cards could not be used (8). Services employees dependent on communications were sent home and businesses that provide networked services to the local agricultural community could not operate. IBM's Silicon Valley lab was shut down, and workers at an IBM manufacturing facility were sent home. The Internet Assigned Numbers Authority (IANA) — which translates between domain names and Internet addresses — lost access to at least one server.


## The Response

Press reporting characterized the response from police, fire, and other emergency workers as swift and smooth. Around 2:00 AM, police in Morgan Hill and Gilroy contacted Santa Clara County dispatchers to report their phones were down. Santa Clara County officials declared a local state of emergency. At 3:50 a.m., Morgan Hill police went to the house of the city's coordinator of emergency services and apprised her of the situation. Also about that time, police woke up the emergency coordinator for the Morgan Hill Amateur Radio Emergency Services (ARES), an organized group of ham radio operators who can supplement law enforcement and emergency response radio communications, and began alerting ARES members. At 5 a.m., the County's coordinator of emergency services was notified and the county activated its Emergency Operations Center. At 5:15 a.m., Morgan Hill's volunteer coordinator of a city program that trains residents in emergency preparedness was alerted (9).

At 7:36 a.m., AT&T sent out its first Twitter message to California customers warning of the outage.

By the time most people started their day in southern Santa Clara County, amateur radio operators had set up alternative communications links for police and fire departments, and for hospitals. Police patrols were increased so that people could flag down officers on the


*U.S. Airman Bryan Payton, a network systems administrator with the 380th Expeditionary Communications Squadron, completes an operational check on a portion of the base's network. (U.S. Air Force photo by Tech. Sgt. Charles Larkin Sr./Released)*

street in an emergency. Police were able to communicate internally via police radio and microwave links. The fire department moved additional firefighters to stations in the affected area, and staff and equipment were positioned at vantage points in the hills to watch for smoke (10). The county sheriff increased staffing and patrols. In addition, the city of Gilroy sent out emergency notifications on a cable news channel and AM radio, and freeway signs directing people to these media outlets were set up (11).

The Morgan Hill Community Emergency Response Team, local volunteers with basic police and medical-response training, was deployed around the city. The Cisco Systems Network Emergency Response Vehicle (NERVE), an emergency communications truck, was dispatched to Morgan Hill and set up satellite communications links to restore phone and Internet service to the police department (12).

Santa Cruz County also responded, going into "operational mode" as it would during any large-scale emergency. Police agencies put as many uniformed officers as possible on patrol. The Sheriff's department sent deputies to the homes of doctors needed at the county's three hospitals; deputies also were sent to check on some known ill or elderly people, while other deputies manned community service centers. Ham operators set up shop in the county's hospitals.

By 2 p.m., one of the San Jose cables was repaired and some service to the south county area had been restored. By 5 p.m., phone service to Morgan Hill, Gilroy, and parts of Santa Cruz and San Benito counties was restored. By 7 p.m., more service was restored; at 9:26 p.m. AT&T sent a Twitter message saying that fiber connections serving Santa Clara and San Jose had been partially restored and most 911 service was back up. All service was restored by 12:15 a.m. Friday, April 10.

## The Implications

As this overview illustrates, the overriding immediate concern was the threat posed to public safety, especially the 911 and medical services. Because this is earthquake country, emergency responders are used to practicing established emergency plans and procedures, and several officials opined that this event was "great training" for the next big quake. The threat of economic losses was considered regrettable but of far less importance, with the notable exception of banks, which police visited in person to recommend closure.

The two main elements of the response were an increase, as much as possible, in the physical presence of law enforcement in the affected areas, and the shift to self-contained radio communications between police and other emergency responders. Key to the success of the latter was the work of volunteer ham radio operators, who

aided and supplemented official and hospital operational communications.

Post-mortem commentaries on the event focused on the need for better physical security and more network redundancy, although a number of writers suggested the threat was overblown and did not warrant major efforts to protect the cable networks.

Many commentators and posters called for greater physical security for fiber optic lines — sealing manhole covers, for example. But these calls were generally met with arguments citing cost and practicality: not only would additional physical security increase network costs, it would significantly hinder access to cables by repair personnel.

A central topic of the post-event discussions was network redundancy. Although details of AT&T's cable infrastructure were not discussed in public, several analysts expressed surprise at the magnitude of the consequences, especially in this technologically advanced region. A Sprint representative said, "Fiber cuts happen more often than people realize ... It happens all the time when people are drilling or digging up the street." (13) Some suggested the perpetrator(s) had inside knowledge of the network structure and may have targeted the cuts to defeat AT&T's apparently limited physical redundancy, or may have known of some ongoing maintenance issue that had temporarily reduced the availability of redundant links. The vulnerability resulting from the consolidation of so much traffic on just a few lines was brought to public and official attention, and the distinction between "virtual redundancy," of providers and channels, and the physical redundancy of the actual communications media was highlighted (14). One report said the Sprint line that was cut in San Carlos did have a separate backup and thus traffic could be rerouted without significant loss of service (15).

The common counter-argument was based on economic considerations. The director for Infrastructure Assurance and Security at the University of Texas at San Antonio said it is possible to add more redundancy to the networks but that doing so could take billions of dollars, a cost that would be borne by subscribers (16). Network administrators generally agreed that market forces have driven the consolidation of communication infrastructure and little can be done to reverse this trend.

Online discussion among network administrators tended to suggest it is the responsibility of individual network operators to ensure the redundancy of their own networks. Administrators for businesses that must have reliable Internet or other WAN access usually purchase service from dual providers, often using a fiber/copper main channel and a fixed-wireless backup. To make sure that their providers are not sharing lines, network designers can purchase commercial telecommunications infrastructure mapping tools, such as FiberSource.

Redundancy via different media/channels was suggested also. One poster in a network administrator discussion group suggested that the incident should prompt the proliferation of WiMAX as an alternative path for Internet and long distance telephony (17). Another alternative medium suggested was microwave backhaul, considered to be less vulnerable than cable because there are no physical lines to cut, the system hardware is mounted high on poles and is therefore difficult to access, and jamming was said to be difficult. However, jamming is possible, wireless links are subject to weather disturbances, and these links need to connect into the fiber backbone at some point anyway. One poster suggested backup laser communications systems could be used as emergency channels in the event of a cable outage. This idea might be practical in a few restricted circumstances but in general, its practicality is reduced by propagation degradation and line-of-sight constraints.

In the end, the consensus — particularly among industry insiders — seemed to be that "backhoes happen" and the consequences of accidental or intentional cable cuts do not justify the cost and inconvenience of additional protection or redundancy. Five days after the incident, one person on the online North American Network Operators Group pretty much closed the conversation with the comment: "fiber cut over, there will be more, move on."

## Lessons Learned

This event provides an instructive contrast to the speculation seen in the IO literature from time to time. On the one hand, writers sometimes suggest that a few knowledgeable attackers can disrupt telecommunications enough to paralyze a nation. On the other hand, writers point to (assumed) communications diversity and redundancy and suggest that any attack on the cables is unlikely to be noticed by anyone but the network operators. This real-world example fell somewhere in between. The consequences were surprisingly severe, but in the final analysis, no real harm was done apart from a day or so of personal inconveniences and unknown economic losses suffered by local businesses.

Given that, what can we learn from this event? The circumstances prompt several questions.

*What are the controlling factors that magnify or limit the effects of such an attack?* Obviously, a key factor is the network layout and communications redundancy in the target area. Many but evidently not all regional networks have multiple fiber rings for redundancy, and some networks have additional redundancy. One article said carriers such as Deutsche Telekom are building mesh networks to provide a third layer of redundancy (18). In addition, independent channels (e.g., a corporation's independent VSAT network) that can pick up the load or support recovery coordination add resilience to the overall communications infrastructure in the region. Network security measures are a related factor; although critical nodes may be protected, the cable lines and vaults often are not.

*U.S. Air Force Senior Airman Santos Rodriguez, a client support administrator with the 28th Mission Support Group tests a computer's power supply unit surge. (U.S. Air Force photo by Airman 1st Class Joshua J. Seybert/Released)*

Another factor is the degree of the target area's dependence on telecommunications, which was high in this case. The trend in the US to rely increasingly on remote network-accessible resources to perform core functions of an enterprise (think of "cloud computing" and "Software as a Service") will only increase this dependence.

The availability of emergency resources is yet another factor. This incident occurred in the Silicon Valley area, which has a relatively rich tax base and a reputation for technical sophistication. So not only does the area have emergency plans, it has the resources to equip and execute those plans. If this incident had happened in another, less economically developed area, it is questionable whether the response would have been as effective.

We may note that telecommunications dependence and resource availability tend to be offsetting factors — the more economically prosperous an area is, the more likely it is to be dependent on modern networked telecommunications, but it also is likely to have both the resources to invest in response programs and the motivation to place a high priority on those programs.

It is clear, furthermore, that network redundancy, usage, and security/response resources make up only part of the picture. Geographic, social, economic, organizational, and personal factors played a large part in the response to and recovery from this attack. California is earthquake country, and many municipalities are prepared to deal with the loss of support infrastructures as the result of a large quake. One wonders whether responders less inured to the prospect of sudden disaster would have had the organizational structure and the experience to act with such effectiveness. One of the striking features of the early news reports on this event, as well as blog and forum posts, is a total absence of any sense of panic. Little confusion was apparent and emergency measures seem to have worked as intended. In a different environment, in the US or elsewhere, the response could very well have been less effective.

*What degree of control does an attacker have over the nature, magnitude, and duration of the effects?* A variety of commentators compared this event to the accidental cable cuts that occur from time to time, but is that comparison entirely valid? Unlike an accident, an attack has a target and an objective. The attacker can target the time and place of the attack or of coordinated attacks, as apparently happened in this case. He also has considerable control over the type of damage inflicted. (Some reports on this event said the cuts were very clean, thus facilitating repair; why the attacker(s) did not attempt more thorough destruction is unknown.) The attacker may know something of the cable layout, including services carried, diversity, and backup alternatives.

An attacker also presumably has an objective, which may range from very general to highly specific. We may suggest examples such as the following:

- Sabotaging the network provider's operations, finances, and reputation.
- Sabotaging the operations and performance of selected entities that rely on that communications path — for example, emergency services, a major infrastructure control center, or a major commercial enterprise.
- Driving communications traffic to a different path, as happened at the outbreak of World War I when the British cut undersea cables serving Germany, to force German international traffic onto radio channels that could be monitored.
- Disrupting telecommunications service in preparation for or support of another action such as a truck-bomb attack.
- Performing what may be considered "diagnostics": a test disruption to identify and calibrate attack effects on telecommunications, their extent, their duration, and the consequent effects on the community.
- Generating general disruption ("network terrorism").

We thus are driven to inquire: by how much can the attacker control or magnify the consequences of the attack, or equivalently, to what extent do conditions outside his control drive and limit those consequences? Clearly, the answer depends on the controlling factors noted above. And they are not limited to the design and operation of the network or even of the entire telecommunications infrastructure — they include also human, geographic, and environmental factors.

*How do we predict or assess such an attack?* It would be instructive to develop an "attack model" as an organized method that incorporates the controlling factors and their interdependencies, to help identify and characterize potential vulnerabilities, identify potential threats, or perform post-mortem analysis of attack responses. Examples of these factors might be:

- Elements of the target network infrastructure: the links and nodes, their virtual and physical redundancy, their roles/functions within the network, alternative links and nodes (and their capabilities to support those roles and functions), protection, security, and monitoring methods.
- Elements of the target environment: the structure of the community (including critical centers and resources); the characteristics of its population; the economic, political, military, and social functions it performs; the telecommunications services it uses and the ways it uses them.
- Elements of the target-area defensive infrastructure: emergency organizations, emergency telecommunications resources, supporting community elements.
- Elements of the attack: motivation/objective, attacker identity, knowledge of the target elements, target type and location, method of access, tools and methods, timing, sequencing of multiple attacks, coordination with other hostile activities.
- Elements of the consequences: effects on the network, area(s) affected, derivative effects on the community, effect duration.

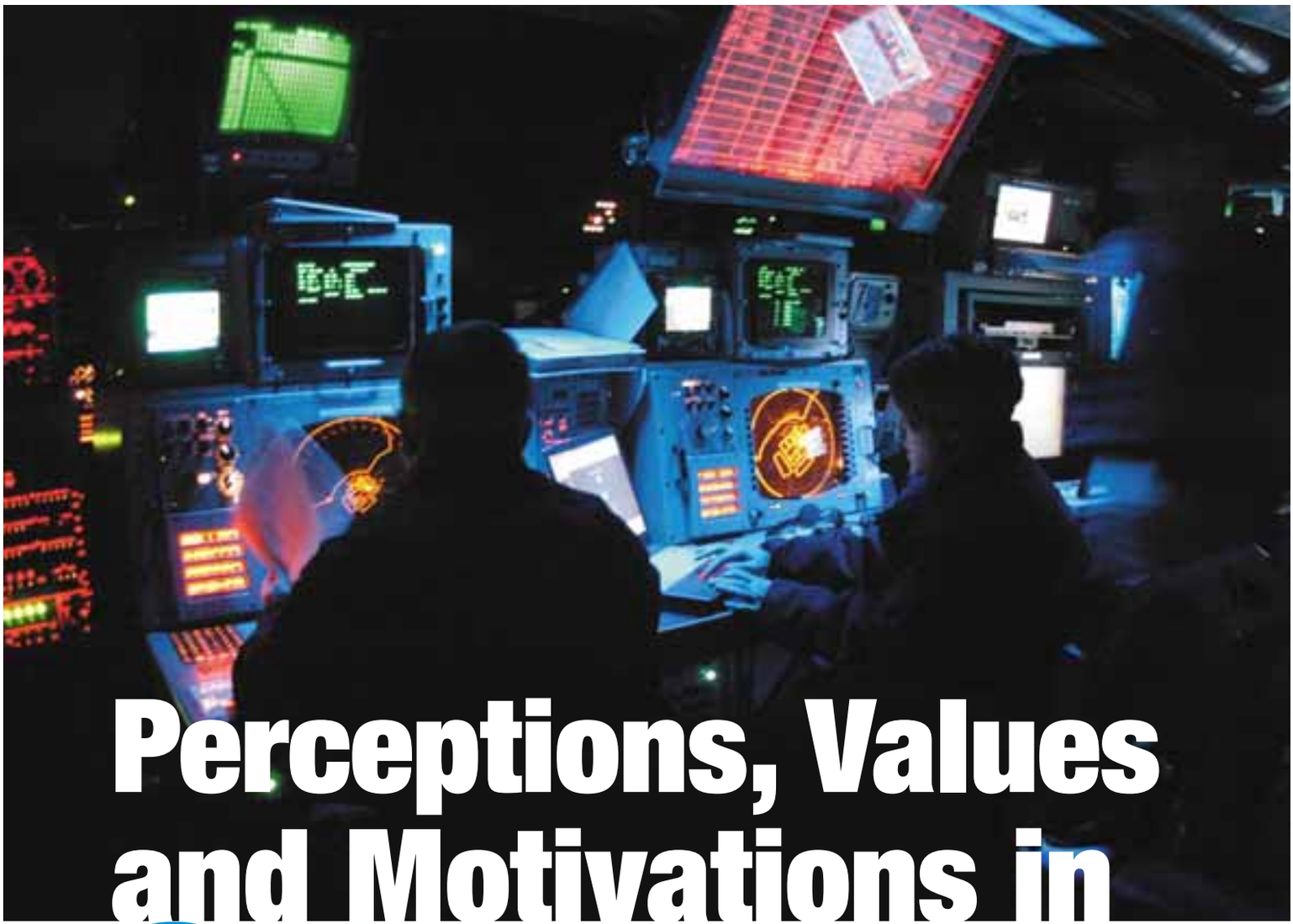
What we wish to emphasize is that any prediction or assessment of an attack on a telecommunications system must treat it not as an attack on the network, but as an attack on a networked social structure. Just as an Information Operations attack is targeted ultimately at an information user or user population, any attack model must assess IO as, ultimately, an attack on the users.

*L. Scott Johnson is a senior engineering analyst at the Sunnyvale, CA office of MacAulay-Brown, Inc. He researches and assesses concepts, methods, and capabilities related to the planning and conduct of all elements of Information Operations.*

*Toni Whyte is a senior analyst at the Sunnyvale, CA office of MacAulay-Brown, Inc. She analyzes IO issues dealing with telecommunications systems and computer networks, with particular emphasis on the social dimension of network warfare.*

**ENDNOTES**

1) Internet, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/10/MNP816VTE6.DTL, page viewed April 2009
2) Internet, http://www.mercurynews.com/topstories/ci_12106300?nclick_check=1, page viewed April 2009
3) Internet, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/10/MNP816VTE6.DTL, page viewed April 2009
4) Internet, http://www.mercurynews.com/topstories/ci_12106300?nclick_check=1, page viewed April 2009
5) Internet, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/10/MNP816VTE6.DTL, page viewed April 2009
6) Internet, http://www.mercurynews.com/topstories/ci_12106300?nclick_check=1, page viewed April 2009
7) Internet, http://sanantoniohams.org/blog/?p=781, page viewed May 2009
8) Internet, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/10/MNP816VTE6.DTL, page viewed April 2009
9) Morgan Hill Times, Ham Radio To The Rescue: Amateur Radio Operators Use Hobby For Service, Michael Moore, April 2009
10) Internet, http://www.morganhilltimes.com/printer/article.asp?c=255181, page viewed May 2009
11) Internet, http://www.mercury news.com/topstories/ci_12106300?nclick_check=1, page viewed April 2009
12) Internet, http://n5fdl.com/davids-blog/2009/4/11/big-win-for-hams-in-silicon-valley.html, page viewed May 2009
13) Internet, http://news.cnet.com/wireless/?keyword=security, page viewed May 2009
14) Internet, http://www.santacruzsentinel.com/ci_12109905, page viewed April 2009
15) Internet, http://news.cnet.com/wireless/?keyword=security, page viewed May 2009
16) Internet, http://www.santacruzsentinel.com/ci_12109905, page viewed April 2009
17) Internet, http://viodi.com/2009/04/12/could-major-telecom-outage-been-prevented-or-alleviated/, posted by Alan Weissberger, April 12, 2009
18) Internet, http://news.cnet.com/wireless/?keyword=security, page viewed May 2009



# Perceptions, Values and Motivations in Cyberspace

**By Christine A.R. MacNulty, FRSA**

To most people, especially physical scientists and engineers, cyberspace is a domain of electro-magnetic frequencies that serves as a medium for communications, control systems and interactive experience. But it is equally a psychological word of individuals and groups, and their interrelationships as they communicate and interact with each other for entertainment, information or political purposes. International relationships, diplomacy, and all forms of warfare are affected by the increasing scope, complexity, ubiquity of, and access to cyberspace.

Over the past fifteen years the impact on warfare from the availability to the general public of information from the World Wide Web, accessed through cyberspace, has been huge. We are all familiar with the scenes from Abu Ghraib that were taken by prison guards, posted on line, and were picked up by the world-wide news media. The devastating impact of those pictures on attitudes of people around the world towards the United States and within the United States is still apparent. Despite its being an isolated incident, it has had far-reaching consequences on all detention facilities.

Despite some religious opposition to the internet, even such groups as the Taliban finally accepted it, saying that they were not against the internet itself,

*Operations Specialist 2nd Class Gretchen Flint along with Operations Specialist Seaman Andrew Wilbanks monitor radar in Combat Information Center (CIC) aboard the amphibious assault ship USS Bataan (LHD 5). (U.S. Navy photo by Mass Communications Specialist 3rd Class (AW) Pedro A. Rodriguez) (Released)*

but only against what was perceived as "obscene, immoral and anti-Islamic material." Cell phone cameras and video-cameras have enabled terrorist groups such as Al Qaeda to conduct information terrorism by transmitting pictures of carnage within seconds of the occurrences — and to blame the US for them — whether or not the US was involved. Subsequent denials by the US with detailed analyses of the situations are less believable to many — including our Allies and fellow Americans — because AQ got there first. People are psychologically disposed to believe information that supports their beliefs and preconceptions, so for those who believe that America is the Great Satan this kind of information (even entirely fabricated information) fuels their anti-American sentiments. Images of Marines holding and caring for babies, or handing out toys or candy cannot improve our image.

If we are to understand the human/psychological domain of cyberspace in order to improve Information Operations, then there are three aspects of it that are important.

- Perception
- Values
- Motivations

## Perception: Is Perception Management possible?

One of the key areas for IO that needs to be researched and understood thoroughly, is that of perception. How do we perceive others, and how do they perceive us? Perception changes all the time — sometimes in a steady trend, other times in steps. We can sometimes anticipate the step changes in a population — as happened with the reports of desecration of the Qur'an at Guantanamo Bay, or the beheading of American civilians — but sometimes tempers flare and we don't know what has caused it. If we are to be able to communicate with, or influence people effectively, we need to be able to understand and measure perception and to deduce *why* it is the way it is, and what the trends seem to be. To be able to understand the *why*, and to use this understanding as the basis for Information Warfare, Strategic Communications and Information Operations, we need a comprehensive picture of *what is happening, why it is happening, and what is likely to happen next.* We also need to decide whether our aim is tactical or strategic. Do we want to influence behavior in the short term (which may not last) or perceptions and attitudes in the longer term.

Influencing perception may be more difficult than we think — and it may be harder in cyberspace than in face-to-face situations. Clinical psychologists know that the frame of mind a person is in influences his perception, because a person sees what he anticipates seeing, and he rarely sees what he has not anticipated seeing. Thus if we are in a bad mood, then we see and understand events and communications through that bad mood, and everything looks bleak. If everything is seen through the lens of strong anti-American feelings, then all of it will add fuel to the fire of that sentiment. If we are in a good mood, then we see things through a lens of good feelings and optimism. We are unlikely to be able to change a person's mood before we communicate with him. However, if we are considering a population, then the population's mood probably forms a normal distribution at any moment — unless we or others have done something to stir up that population for good or ill. Therein lies one possibility for IO, SC or some sort of soft intervention. If we can create a sense of goodwill by frequent, positive, interventions that are designed to affect mood and perception, then we may be able to have greater long-term influence on the population.

## Inter-Cultural Communication in Cyberspace

Research by Reeder, MacFadyen, Roche and Mackie (1) has suggested that while intercultural communication is always a challenge, it is even more of a challenge online in the absence of visual and oral cues, or well-developed relationships. Individuals may hold widely different expectations of how to establish credibility, exchange information, motivate others, give and receive feedback or critique/evaluate information. Tim Jordan (2)

*U.S. Air Force Master Sgt. Vickay Stearns, from the 282nd Combat Communications Squadron, Rhode Island National Guard, works on her computer during Exercise Amalgam Dart, at Camp Rilea, Ore. (U.S. Air Force photo by Tech. Sgt. Sean M. Worrell/Released)*

*US Military personnel assigned to the 4th Psychological Operations Group (POG), 193rd Special Operations Wing (SOW), Pennsylvania Air Nation Guard (ANG) broadcast television and radio programming from onboard an ANG EC-130J Hercules.*

writing in 2000, said that the preconditions of cyberculture usually involve the linguistic and communications norms of Anglo-American societies. He was obviously critical of them, as he went on to say "in which the aggressive, competitive individual is enshrined." Whether that is as true now as nine years ago, we don't know, but we suspect it is.

As a simple example of frequent poor communications, let us consider email where there are few audio-visual cues. While some of these cues can be inserted through the use of emoticons, there are still many opportunities for misunderstanding. How many of us have had friends or colleagues misunderstand and become angry over what we wrote in an email — even when we have an existing relationship and are of the same culture and educational level?

Gudykunst's Anxiety/Uncertainty Management Theory (3) may apply here. He postulates that all communicators, including online communicators, encounter each other as strangers. The wider the cultural gap between them, the greater are the levels of anxiety and uncertainty experienced by them. And as anxiety increases, so does the potential for miscommunication. Most people can "manage" their anxiety to some degree to enable better communication, but even that approach to management has cultural biases. Gudykunst says that in self-introductions, for instance, individuals provide information about themselves in ways that reflect their group cultural programming, their education and experiences. But the likelihood is that the people to whom they are introducing themselves do not have the same expectations of the information given, or the manner of delivery. Thus the mismatch can tend to add to the anxiety rather than diminishing it. If the communicators have different native languages, even though they may be communicating in English (the lingua franca of the internet,) this can add to the anxiety experienced. And anxiety and miscommunication can become a source of anger, in which feelings and emotions can get ratcheted up, even when people want to understand each other. When they are already suspicious of each others' motivations and behavior, then this can fuel their antagonism.

Olson (4) and Dudfield (5) (among others) make a linguistic distinction between oral and literate use of language that could be important for online communications. They have suggested that online communication is a hybrid of both oral and literate language. In addition, online communication is also a mixture of language and pictures suggesting a visual literacy that will, indeed, be culture-dependent.

If we are to mold perceptions (and we prefer that to "manage perception") then we need to be thoroughly familiar with the levels of these various forms of literacy that target populations have, the expectations they have, and the cues that can trigger their supportive or antagonistic behavior.

## Targeting — Real People or Avatars?

IO can be undertaken at strategic, operational and tactical levels, and can play out over different time periods. We need to plan our IO campaigns at all three levels, and in such a way that we target people appropriately — which includes perception molding. This raises a question of who do we target and how in cyberspace? And do people perceive things differently when they are received from media that involve cyberspace? Anecdotal evidence suggests that young people are likely to believe what they see on the internet, or get in text messages from cell phones. Young people around the world tend to "live" in a world of cyberspace — the internet, online games, cell phones, texting — and their cyber-personalities can be quite different from their real life ones. We have heard some debate about whether IO should be targeted to real personalities or to the online/avatar personalities, as if this is a new phenomenon. However, this is not so different from the world outside the internet. People have always exhibited different personalities in different aspects of their lives. Tough guys at work can become mild and loving husbands/fathers at home. Teenagers can exhibit bravado and be rebels at home, but be honor students in schools. Advertising agencies have never had problems advertising to these different personalities. They either advertise to the predominant types for the appropriate contexts (office or home) or they advertise to the most aspirational aspects of a persona. From the perspective of several psychological theories — Maslow, Schwartz, for instance — everyone is aspiring to be "better" in some way. People with sustenance values want more safety and security; people who have strong

esteem values generally want to be wealthier, more powerful and to be see to be those things; people who are moving towards self-actualization tend to want to have better relationships with other people and to know themselves better. Advertising agencies have found that it is more effective to target their advertising *towards where people want* to be than to where they are.

Online personalities/avatars seem to us to be the aspirational aspects of real personalities (in some of these cases, the aspiration may be to be bigger and badder than others, rather than better, but it is still an aspiration.) Thus messages targeted to avatars may reach them more effectively than those oriented to the real person.

## Values & Motivations

Cultures are composed of many different elements, but the key ones we use are values, beliefs and motivations. The objective of our cultural analysis is to sort the population into target subgroups based on those values, beliefs and motivations. Since values underpin motivations, we focus on the core set of values that might compel or influence a group that holds a particular set of values. We can segment the population according to the different values particular subgroups hold. We call these segments personae.

Our instrument for determining cultural values is the face-to-face survey of 21 values-based questions (Shalom Schwartz's Values Portaits (6)) plus other cognitive, attitudinal and behavioral questions. We perform statistical analyses on the results to arrange the responses within the space of all possible responses. We then identify outlier values — what we call "hot" and "cold" buttons — that distinguish each of the subgroups, and we use these values as a basis for crafting the appropriate messages for the subgroup. Then, cross-tabulating the values with the cognitive, behavioral and other relevant questions provides a very rich picture that enables us to flesh out the messages, select the appropriate tone, and select media that appeal to that particular subgroup.

## The Rationale for Using Values

Values are beliefs that are tied inextricably to emotion — not objective, cold ideas — and, as such they operate largely subconsciously. Values underpin a person's motivations, so by understanding a person's constellation of values — both positive and negative ones — we can learn how to motivate him. They serve as standards and criteria for choices and decisions of all kinds. They are ordered by importance relative to one another. Finally, the most powerful way to influence people's behaviour is through values and motivation in a cultural context.

## "Richness" Criterion

When targeting subgroups within a population, it is necessary to have a rich picture of each group so that the targeting, and the basis on which messages are developed, can be as precise as possible. In addition to values, it is always useful to consider many characteristics of the target group. For instance we may need to "slice and dice" the target subgroup/persona by age, gender, tribe, educational levels, urban versus rural, wealthy versus poor, by attitudes, and even by behavior such as media and internet usage. If we have too few values questions or related concepts, we will not have the richness to permit precise targeting. Some academic cross-cultural values studies have focused on major similarities and differences across cultures, and have not focused on the details within a culture. It seems to us that, if we intend to conduct effective operations within and across cultures, then we need to have the richness of the personae, not the simplicity of pure cross-cultural analysis.

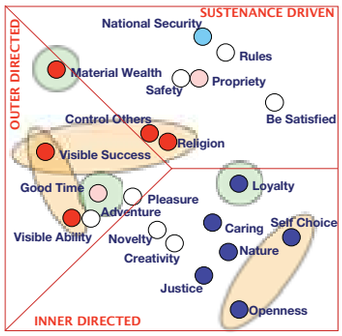
We have conducted a project to identify various "personae" or segments in a particular culture. In that project we focused on young males who might be susceptible to becoming terrorists or supporting terrorists.

For these young males, we were able to develop a typology of 6 groups or personae (Px) . These kinds of personae can be developed for any country, culture, tribe or group. An example of the values of one of these personae (P1) is given in **Figure 1**.

The figure represents what we call a "values space." It shows how the persona feels about values like justice or wealth. The space is segmented with a version

*U.S. Navy Information Systems Tech. 2nd Class Ryan Allshouse uses the intrusion detection system (IDS) to monitor unclassified network activity from the automated data processing workspace aboard aircraft carrier USS Ronald Reagan (CVN 76) in San Diego. IDS is part of the integrated shipboard network system and serves as an important computer network defense enabler, protecting the unclassified shipboard network from cyber attack. (U.S. Navy photo by Rick Naystatt/Released)*

**VALUES MAP OF ONE PERSONA P1**




**"Hot" Button Values**

- It's important for me to have lots of money and material things.
- It's important for me to be seen as successful. I like to impress other people.
- I need to show my abilities. I really want people to admire me for what I do.
- It's important for me to be in charge and tell others what to do. I want people to do what I tell them.
- Religious belief is important to me. I try to do what my religion requires.
- It's important to have a good time and I like to "spoil" myself.
- It's important to me to always behave properly. I want to avoid doing anything people would say is wrong.

**"Cold" Button Values**

- I'm not hung up on making my own decisions about what I do. Freedom to choose and plan my own activities is over-rated.
- I think people make too much of the equality thing. Nothing says the world has to be fair – and, anyway, I'm not going to worry about justice for people I don't know.
- I really don't think I should have to listen to, or try to understand people who are different than me. If they don't agree with me – well, that's up to them.
- Taking care of the environment is another of those overplayed issues. Nature can take care of itself.
- I don't feel a particular need to help others around me. I'm not driven to care for other people.
- It's not important to me to be loyal to my friends. I don't have any need to devote myself to people around me.
- National security is not a big issue for me. I'm not concerned that social order should be protected.

**Motivations pro/con foreign fighters**

**Main inhibitors to supporting foreign fighters are a rather selfish self-interest (desire for wealth combined with a disregard for loyalty), and the desire to have a good time.**

**Motivated to support foreign fighters by a strong drive for visible success/ability and a desire to control others. Also motivated by the need to follow and fear of "the other".**

of Maslow's hierarchy. The red/pink and blue/pale blue dots represent the values on which this particular persona is statistically significantly above or below average. Next to the values space is a first person expression of the particular values about which the persona is either "hot" or "cold." We interpret the particular combination of hot and cold buttons to build a detailed values profile of the group. In addition, these hot and cold buttons map to value statements, which can help craft messages that "push" those hot or cold buttons.

We examine the patterns of hot and cold buttons in a subgroup to assess whether or not they can be pushed to reduce support for terrorism. For example, Material Wealth, a desire to have a Good Time in life and a rejection of Loyalty mitigate against the young men of this persona (P1) joining any group that cannot provide for these needs. We also note that there are buttons our adversaries could push to increase support for terrorism among the target group. We assess that a combination of Visible Success and Ability, Controlling Others and Religion, together with a rejection of Openness, might motivate this subgroup to become terrorists in countries where they are unlikely to be able to satisfy their needs for material wealth and good times. Indeed, this is a "risky" group in many different cultures. In a project for a British financial institution, several young men from this kind of persona were among the most active money launderers.

We then interpret the values space — the values themselves, their relationships to one another, and their cross-tabulations with other attitudinal and behavioral questions — to provide detailed understanding of the messages that will appeal to each persona, the content, tone and media that they are likely to use. For example, messages to this particular group (P1) need to stress visible success and ability in directions other than terrorism and, if possible, the ability to increase wealth and the means to have a good time. The messages need to be future-oriented and emotional, not logical. Ethics and morality are not relevant to them, and references to Loyalty, Social Justice, Caring, and Openness would turn them off.

There is nothing magical about 6 personae. We could expand the number of personae if we wished to have a more precise method for targeting a particular audience, or contract the number if we wanted a strategic overview.

It is worth noting that we use the same 21 Schwartz values for whatever country we are examining, but the values space will be slightly different for each country based on the responses to the questions and the subsequent factor analysis, and the personae will exhibit different hot and cold buttons.

## Cultural-Cognitive Dimensions — Us versus Them

There is one more area that is critical if we are to communicate effectively, and that is an understanding of the major differences between those of us who are trying to do the influencing and the recipients of our communications. Some of those differences are based on values, some on tradition and some on general cultural characteristics.

We are concerned that, in many cases, we Americans and even Europeans (who are more used to operating in different cultures) are not sufficiently introspective to understand ourselves and "where we are coming from" to use a popular phrase. That makes it even more difficult to understand where other people are "coming from" — what their perspectives are and how far removed those perspectives are from ours. If we are to learn to communicate effectively with any other culture, then we need to know where we (Americans and Europeans) are on these dimensions, and where the people to whom we are communicating are placed. If there are significant gaps between us and them on any particular dimension, then we know we need to be very careful about the way we communicate, the words and phrases we use, the actions that we are asking them to perform and the time frames we are wanting to put in place.

We have identified 17 cultural dimensions that we believe are important to understand, if we are to communicate effectively with other cultures. I have described eight of these in detail here.

### *Values, Beliefs, and Motivations* (sustenance driven to self actualization)

On one side of the continuum are cultures that are sustenance driven. They are concerned with meeting their basic needs and, even when they have the things they need for survival, they

tend to focus on holding on to what they have, including tradition. In contrast, self-actualized cultures (and people) are not focused on basic survival needs. They are driven by intrinsic goals. They place more importance on personal accomplishment (such as a career, or relationships) and on people than they do on material things. Middle aged Westerners tend to be on the Self Actualized side of Esteem, while Middle Eastern leaders are on the Sustenance Driven side of Esteem, and the general populations are Sustenance Driven

### *Epistemologies — the Way we Know things* (authority-based to empirical)

We, in the West, have adopted an empirical, scientific approach to how we know things. We use the scientific method—positivism, objectivism, and reductionism. We analyze things, break them into component parts, and reassemble them. In some non-Western countries, the way of knowing things is much more authority-based. The Qur'an is the prime source of knowledge for Muslims. Muslims use it and the Hadith to make sense of their situations. Since this kind of "knowing" seems superstitious to many in the West, we do not even know how to go about understanding the Muslim approach to knowing. If we do not share epistemologies, then this is the first dimension that we need to consider when dealing with another culture.

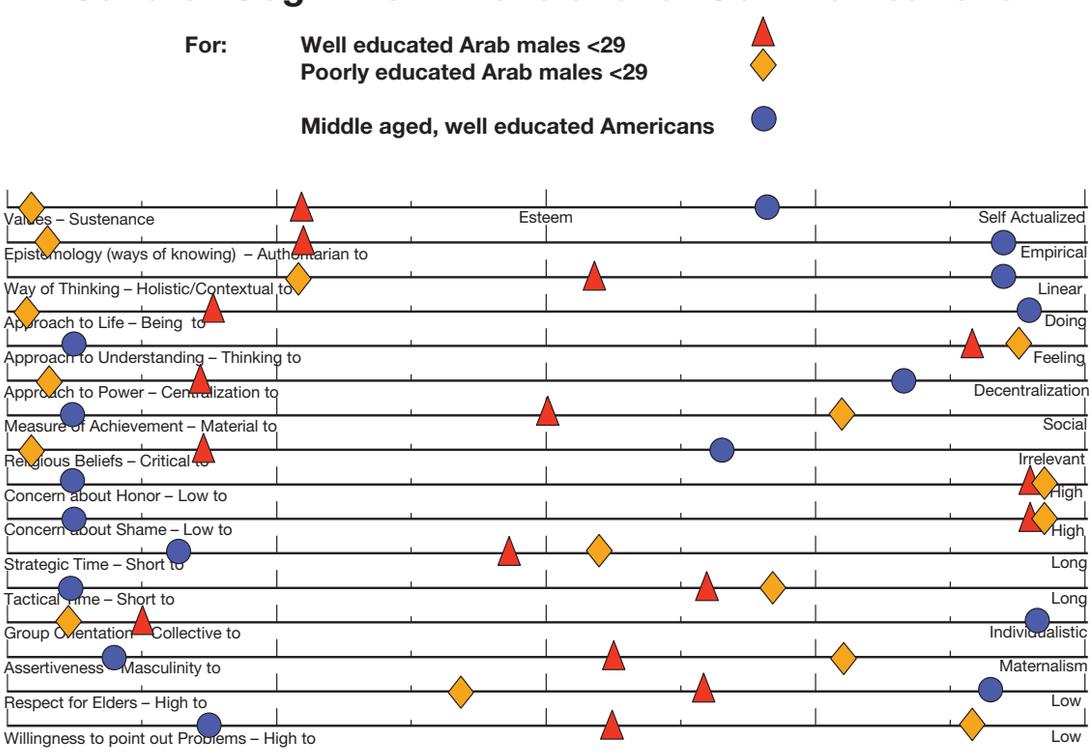
### *Ways of Thinking (7)* (linear to holistic)

This dimension has great importance to us, since we in the West (and particularly the United States) have a very linear, rational (Cartesian) approach to thinking. We pride ourselves on our analytical capability and our ability to separate out logic from emotion. In doing so, however, we often ignore contexts and the interdependencies that are of critical importance to other cultures. Indeed we find it difficult to imagine how people who think holistically operate. Yet cultures in the Far East tend to have a much more holistic way of thinking. Cultures in the Middle East seem to be somewhere between the two. We would consider this to be the next dimension that we should understand when communicating with other cultures. An interesting anecdote here comes from a software house that employed programmers and systems analysts from several cultures, but all of whom had spent some time in US or British universities. All of them produced excellent programs. But when it came time to de-bug the new programs, the British and American members of the teams had no problem de-bugging each others' code, but they couldn't follow the logic trails of those from India or Pakistan — and vice versa.

### *Approaches to Life* (being to doing)

This may seem like a peculiar notion to Americans, who are inveterate do-ers. But there are parts of the world, both

## Cultural-Cognitive Dimensions for Communications



Middle and Far East, where the society has a much greater acceptance of what is, and very little inclination to change it. In the Middle East, the phrase *"If it be the will of Allah"* is used constantly, and events and circumstances are just accepted without the kind of questioning that Americans would indulge in. As a result we too often try to force issues far too fast for the people of those regions. An illustration of this is the American tendency to try to avoid or speed up the process of sitting down with Middle Eastern or Asian counterparts to drink tea. To Americans the process is a waste of time; they should be getting on with business. To the others, it is a process of becoming comfortable with the Americans — as they do with all guests — and not conducting business until they feel in harmony.

### *Approaches to Understanding* (thinking to feeling)

In the West, with our linear approach to thinking and our empirical epistemology, we have an intellectual approach to understanding. We expect to be able to analyze things intellectually, and we pride ourselves on being objective. This contrasts with Middle and Far Eastern cultures that place a much higher value on feelings and emotions, and that expect people to speak about and show their emotions. In conversation with two Egyptians, they said that they could not make a good decision without bringing emotion — the way they feel — into it. Thus we need to be willing to show emotion more in dealing with such cultures, and even bring emotion into our negotiations.

### *Concern about Honor* (low to high)

This and the next dimension are related to Values and Motivations, but I believe that they are important enough to be called out separately. Honor is of great importance to everyone in the Middle East and Far East, and it is a critical value for individuals, families, tribes, and nations. In contrast, outside the Armed Forces, in the West the concept of honor has all but disappeared. Thus we do not pay anywhere near enough attention to this value in our dealings with people of other cultures. If we are to influence them, we need to ensure that they are able to maintain dignity and honor.

### *Concern about Shame* (low to high)

This dimension is the opposite of honor, but because it is so critical in its own respect, I consider it to be a key dimension. People in both the Arab Middle East and the Far East are very concerned with "saving face" and not bringing shame to oneself or one's family. In the West, the concept of shame has almost disappeared. I have heard people discussing the idea that we should make fun of, or otherwise humiliate our adversaries. While that might work with some, it seems to me that it is more likely to harden radicals in their opposition to us.

### *Strategic Time* (short to long)

This dimension is about a culture's sense of history and the understanding brought about by that sense of history. It permeates every story, every perception, and every decision. It is also about the time over which they expect their actions to play out. In the United States, we have probably the shortest strategic time of anywhere on the planet, and this can be seen in our desire for everything to happen "right now." This can be a real handicap for the US in areas where we expect to see results, as those with whom we are negotiating will have different expectations of a "reasonable" time.

## Conclusions

We will not succeed in Information Operations if we rely only on demographic and behavioral information, and if we use a shotgun approach to broadcasting messages. Understanding Perceptions, Values and Motivations can be a force multiplier in IO, by providing the mechanism for much more precise formulating and targeting of messages. Whether we have to resort to rumor-mongering in person in countries with little access to radio, television or the internet (some parts of Africa, for instance) or whether we plan to use cyberspace, the more we know about segments in the population, what values they hold, and what motivates them, the more successful we will be.

*Christine MacNulty, President & CEO of Applied Futures, has 40 years experience as a consultant in long-term strategic planning for concepts as well as organizations, technology forecasting, technology assessment and related areas, as well as socio-cultural change. For the last 15 years, most of her consultancy has been conducted for the Department of Defense. During the last 30 years Christine MacNulty has contributed methods and models for understanding social and cultural change. She developed the European version of SRI International's Values & Lifestyles Program, and worked with the International Research Institute on Social Change to develop their social models for use by industry. She has applied her knowledge of people and their values and beliefs to strategic planning, marketing planning, advertising, vision development, organizational change, R&D planning, new concepts, technology assessment and business development.*

**ENDNOTES**


1) Reeder, MacFadyen, Roche and Mackie, "Negotiating Cultures in Cyberspace: participation patterns and problematics," *Language, Learning & Technology*, May 2004
2) Tim Jordan, "Language and Libertarianism", *Sociological Review, 49(1), 2001*
3) Gudykunst, "Anxiety/Uncertainty Management Theory" in Wiseman's *Intercultural Communication Theory,* Sage, 1995
4) Olson, *The World on Paper: The conceptual and cognitive implications of writing and reading,* Cambridge University Press, 1994
5) Dudfield, *Literacy and Cyberculture,* Reading Online, July 1999. (www.readingonline.org)
6) Schwartz, Shalom; Melech, Gila; Lehmann, Arielle; Burgess, Steven; Harris, Mari; Owens, Vicki, "Extending the cross-cultural validity of the theory of basic human values with a different method of measurement," *Journal of Cross-Cultural Psychology. 2001 Sep Vol 32(5)*
7) Richard E. Nesbitt, *The Geography of Thought,* The Free Press, NY, 2003

# Join the AOC's IO Institute

## Benefits of IOI and AOC Individual Membership:

- *The IO Journal* – the premier professional journal of Information Operations.
- Through our worldwide chapters, access to an extensive network of government and industry professionals in the fields of Information Operations and related and supporting fields.
- Excellent networking opportunities:
    - Through chapter and regional activities tailored to meet local professional development needs.
    - Through world-renowned national/international conventions, exhibitions, conferences and symposia sponsored by the IOI and AOC.
- Career strategy assistance:
    - Access to job postings by IOI and AOC corporate members.
    - Access to the IOI and AOC's Professional Development Center – advanced education and training in communications, intelligence and information systems disciplines.
- Awards and scholarship programs for recognition of professional and academic accomplishments.

**Visit www.crows.org and click "Join the AOC IO Institute" for an application.**

AOC
Association of Old Crows

# New Beginnings Bring New Challenges

With the new network-centric solutions needed to keep America safe, there will be many challenges. We have the right people to address them. We're Science Applications International Corporation — 45,000 smart, dedicated people who have the deepest understanding of their fields and a passion to find the right solution.

No job is more important to us than keeping America safe, and we take pride in knowing that we're trusted to make a difference. Designing safe network-centric solutions and keeping networks and critical infrastructure running to protect our country against threats are just a few of the missions we take to heart every day. Smart people solving hard problems.

For detailed information, visit us at **www.saic.com**

Energy | Environment | National Security | Health | Critical Infrastructure

SAIC®
From Science to Solutions



10-0186